ConneXium
Ethernet-Verkabelungssystem
Switch-Verwaltungshandbuch

Version 3.0

35001898 03

a brand of Schneider Electric

Telemecanique

Inhaltsverzeichnis

Sicherheitshinweise 5

Über dieses Buch 7

Kapitel 1 Einleitung 9
Auf einen Blick. 9
Industrielle Netzwerklösungen mit Zukunft 10
ConneXium Fast-Ethernet-Switches 11

Kapitel 2 Hardware 13
Auf einen Blick. 13
ConneXium-Switch 499NESx7100 14
ConneXium-Switch 499NOSx7100 15

Kapitel 3 Installation und Inbetriebnahme 17
Auf einen Blick. 17
Sicherheitsinstruktionen 18
Installation von Geräten 20
Inbetriebnahme 27
Grundeinstellungen 28
TFTP-Server für Software-Aktualisierungen 39
Systemmonitor 1 44
Systemmonitor 2 48

Kapitel 4 Funktionen 51
Auf einen Blick. 51
Hardware-Funktionen 52
Anzeigen 53
Datenblockvermittlung. 54
Redundanz 55
GMRP 59
Sicherheit und SNMP-Traps 61

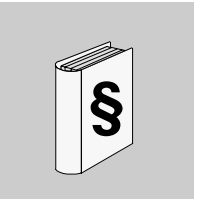
Kapitel 5 Webbasierte Verwaltung 65
Auf einen Blick 65
Starten der webbasierten Schnittstelle 66
Funktion der webbasierten Benutzeroberfläche 69

Kapitel 6 Verwaltungsinformationsbasis (MIB). 79
Auf einen Blick 79
Verwaltungsinformationsbasis (MIB) 80
MIB II 83
Private MIB 95

Kapitel 7 Benutzerschnittstelle. 99
Auf einen Blick 99
Benutzerschnittstelle starten (NxS07100) 100
Arbeiten mit der Benutzerschnittstelle (NxS07100) 102
Starten der Benutzerschnittstelle (NxS17100). 107
Arbeiten mit der Benutzerschnittstelle (NxS17100) 109

Index 119

Sicherheitshinweise



Wichtige Informationen

HINWEIS

Lesen Sie diese Anweisungen gründlich durch und machen Sie sich mit dem Gerät vertraut, bevor Sie es installieren, in Betrieb nehmen oder warten. Die folgenden Hinweise können an verschiedenen Stellen in dieser Dokumentation enthalten oder auf dem Gerät zu lesen sein. Die Hinweise warnen vor möglichen Gefahren oder machen auf Informationen aufmerksam, die Vorgänge erläutern bzw. vereinfachen.

Erscheint dieses Symbol zusätzlich zu einem Warnaufkleber, bedeutet dies, dass die Gefahr eines elektrischen Schlags besteht und die Nichtbeachtung des Hinweises Verletzungen zur Folge haben kann.

Dies ist ein allgemeines Warnsymbol. Es macht Sie auf mögliche Verletzungsgefahren aufmerksam. Beachten Sie alle unter diesem Symbol aufgeführten Hinweise, um Verletzungen oder Unfälle mit Todesfolge zu vermeiden.

GEFAHR

GEFAHR macht auf eine unmittelbar gefährliche Situation aufmerksam, die bei Nichtbeachtung **unweigerlich** einen schweren oder tödlichen Unfall oder Beschädigungen an Geräten zur Folge hat.

WARNUNG

WARNUNG macht auf eine möglicherweise gefährliche Situation aufmerksam, die bei Nichtbeachtung **unter Umständen** einen schweren oder tödlichen Unfall oder Beschädigungen an Geräten zur Folge hat.

VORSICHT

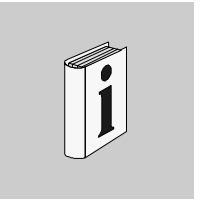
VORSICHT macht auf eine möglicherweise gefährliche Situation aufmerksam, die bei Nichtbeachtung **unter Umständen** einen Unfall oder Beschädigungen an Geräten zur Folge hat.

BITTE BEACHTEN

Elektrische Geräte dürfen nur von Fachpersonal gewartet und instandgesetzt werden. Schneider Electric haftet nicht für Schäden, die aufgrund der Verwendung dieses Materials entstehen. Dieses Dokument ist nicht als Betriebsanleitung für nicht geschultes Personal vorgesehen.

© 2003 Schneider Electric Alle Rechte vorbehalten

Über dieses Buch



Auf einen Blick

Ziel dieses Dokuments

Schneider Automation liefert eine komplette Produktfamilie mit einheitlicher Verwaltung über Lichtwellenleiter-Schnittstellen/elektrische Schnittstellen für Feldbussysteme durch Ethernet-Transceiver, Hubs, Switches und Fast Ethernet ConneXium-Switches. Dieses Handbuch gilt für Firmware Version SV:2.x bei Geräten vom Typ 499NES07100 und 499NOS07109 und für Version SV:4.0 bei den verwalteten ConneXium-Switches vom Typ 499NES17100.

Gültig-keitsbereich

Die in diesem Handbuch enthaltenen Informationen, Daten und Abbildungen sind nicht verbindlich. Wir behalten uns das Recht vor, unsere Produkte entsprechend unserer Politik der kontinuierlichen Produktentwicklung zu ändern. Die in diesem Handbuch enthaltenen Informationen können ohne vorherige Benachrichtigung geändert werden und sind als nicht verbindliche Informationen von Schneider Electric zu betrachten.

Weiterführende Dokumentation

Titel	Referenz-Nummer
Benutzer- und Planungshandbuch für Transparent Factory	490USE13302
ConneXium Ethernet-Verkabelungssystem: Kurzübersicht	Im Lieferumfang von Switch-Produkten enthalten

Produkt-bezogene Warnhinweise

Schneider Electric übernimmt keinerlei Verantwortung für Fehler, die in diesem Dokument vorhanden sein können. Wir bitten um Benachrichtigung, wenn Sie Vorschläge für Verbesserungen oder Ergänzungen haben oder wenn Sie Fehler in dieser Publikation gefunden haben.

Kein Teil dieses Dokuments darf ohne die ausdrückliche schriftliche Erlaubnis durch den Herausgeber Schneider Electric in irgendeiner Weise oder mit irgendeinem Verfahren elektronischer oder mechanischer Art, auch nicht durch Fotokopieren, vervielfältigt werden. Alle Rechte vorbehalten. Copyright 2002.

Bei der Installation und der Verwendung dieses Produkts müssen alle relevanten staatlichen, regionalen und lokalen Sicherheitsbestimmungen eingehalten werden. Aus Sicherheitsgründen und um die Übereinstimmung mit dokumentierten Systemmerkmalen zu gewährleisten, sollten Reparaturen an Komponenten nur vom Hersteller vorgenommen werden.

Wenn Steuerungen für Anwendungen mit technischen Sicherheitsanforderungen eingesetzt werden, sind die relevanten Anweisungen zu beachten.

Der Einsatz von Software, die nicht von Schneider Electric stammt oder von Schneider Electric genehmigt wurde, in Verbindung mit unseren Hardware-Produkten, kann zu Verletzungen, Schäden oder fehlerhaften Betriebsergebnissen führen.

Die Nichtbeachtung dieser produktspezifischen Warnung kann Körperverletzung oder Materialschaden zur Folge haben!

Benutzer-kommentar

Ihre Anmerkungen und Hinweise sind uns jederzeit willkommen. Senden Sie sie einfach an unsere E-mail-Adresse: TECHCOMM@modicon.com

Einleitung

1

Auf einen Blick

Übersicht

Schneider Automation stellt eine neue komplette Gruppe von innovativen Ethernet-Produkten zur Unterstützung von Ethernet-Architekturen mit Echtzeitfähigkeiten und hoher Verfügbarkeit vor. ConneXium ist eine komplette Produktfamilie mit einheitlicher Verwaltung von Lichtwellenleiter-Schnittstellen/elektrische Schnittstellen für Feldbussysteme über Ethernet-Transceiver, Hubs, Switches und Fast Ethernet ConneXium-Switches - Schneider Automation liefert all diese Produkte aus einer Hand!
Dieses Handbuch gilt für Firmware Version SV:2.x bei Geräten vom Typ 499NES07100 und 499NOS07109 und für Version SV:4.0 bei den verwalteten ConneXium-Switches vom Typ 499NES17100 und 499NOS17100.

Inhalt dieses Kapitels

Dieses Kapitel enthält die folgenden Themen:

Thema	Seite
Industrielle Netzwerklösungen mit Zukunft	10
ConneXium Fast-Ethernet-Switches	11

Industrielle Netzwerklösungen mit Zukunft

Übersicht

Die Unterstützung von Trends in der Automationstechnologie und Prozesssteuerung bedeutet eine Bewegung hin zu offenen, transparenten Systemlösungen. Diese stützen sich in zunehmendem Maße auf eine offene SPS-Steuerung mit Ethernet- oder Intranet-Zugriff. Die wichtigsten Standards sind TCP/IP-Kommunikationsprotokolle, Ethernet-Netzstrukturen und Modbus als industrieller Anwendungsprotokollstandard. Viele Steuerungen, SPSs und DCSs (Distributed Controller Systems, Dezentrale Steuersysteme) haben bereits eine Ethernet-Schnittstelle. Schneider Automation liefert bereits Lösungen für dezentrale Steuerungen, Feldbus- und E/A-Lösungen, die auf Ethernet und unseren Modicon TSX-Produktgruppen basieren.
Obwohl der in der Automationstechnologie verwendete Ethernet-Standard derselbe wie in Ämtern und Büros ist, unterscheiden sich die Erfordernisse für Netzwerkprodukte erheblich. Bei täglich zum Einsatz kommenden industriellen Anwendungen wird vorausgesetzt, dass Netzwerke unter extremen Bedingungen - beispielsweise elektromagnetische Störungen, hohe Betriebstemperaturen und starke mechanische Belastungen - zuverlässig funktionieren.

Verfügbarkeit

Die Produktfamilie ConneXium Fast-Ethernet-Switch wurde unter Berücksichtigung all dieser Anforderungen speziell zum Einsatz in Anwendungen der industriellen Automation entwickelt. Der entsprechend diesen Erfordernissen entwickelte redundante "Ethernet-Ring" von Schneider Automation gewährleistet selbst dann einen kontinuierlichen Produktionsbetrieb, wenn das Netzwerk neu konfiguriert wird. Der "Ethernet-Ring" ermöglicht außerdem, dass Netzwerke verwaltet und erweitert werden können, während sie in Betrieb sind. Da das System in Sekundenbruchteilen neu konfiguriert wird, ist der "Ethernet-Ring" bedeutend schneller als der Spanning-Tree-Algorithmus, der nur die Erfordernisse der Bürotechnik erfüllt.
Der "Ethernet-Ring" und andere Konzepte gewährleisten eine maximale Zuverlässigkeit des Netzwerk- und Produktionssystems. Unsere hochintegrierte Familie von Ethernet-Produkten ermöglicht jederzeit die Anpassung Ihres Netzwerks an die spezifische geografische Konfiguration und die Realisierung von Sicherheitsvorkehrungen. Durch die gegebene Skalierbarkeit kann das Netzwerk auch zukünftige Erfordernisse erfüllen.

Merkmale

Allgemeine Merkmale sind:
- hoher Temperaturbereich, der neue Anwendungsfelder zuläßt,
- schnelle Installation (die robusten Geräte werden einfach an einer Standard-DIN-Schiene angebracht),
- einfache Steckverbindungen und umfassende Statusanzeigen, die während der Installation Zeit einsparen.

ConneXium Fast-Ethernet-Switches

Übersicht

Da sie von Anfang an von Schneider Automation als auftragskritische Switches konstruiert wurden, haben die ConneXium Fast-Ethernet-Switches den Vorteil, dass keine einzelne Komponente weder physikalisch noch logisch einen Ausfall des gesamten Netzwerks verursachen kann, wenn die Switches in einer "Ring-Topologie" konfiguriert sind. Durch eine hohe Elastizität im Betrieb sorgen die Switches für ein "kugelsicheres" Ethernet-Netzwerk.

Je nach Wichtigkeit der Prozessanwendung kann die Elastizität im gesamten Netzwerk angepasst werden, um weitere Kontinuitätserfordernisse zu erfüllen. Wenn eine Steuerung beispielsweise zwei redundante Netzwerkkarten hat, kann jede Karte mit separaten Switches im gleichen elastischen Lichtwellenleiter-Ring verbunden werden. Wenn eine doppelte Redundanz benötigt wird, kann ein zweiter Ring hinzugefügt werden.

Die Fast-Ethernet-Switches der Reihe ConneXium NxS ermöglichen eine einfache und kosteneffektive Konfiguration von mittleren bis großen deterministischen Ethernet- bzw. Fast-Ethernet-Netzwerken. Ein wichtiges Merkmal dieser NxS-Switches ist die schnelle Medienredundanz. Der Ausfall eine Übertragungspfads wird in weniger als 500 ms erkannt, und der Switch leitet die Daten auf einen redundanten Pfad um. Sie können diese Funktion über DIP-Schalter an jedem Switch aktivieren. Dieser NxS-Switch von Schneider Automation gewährleistet eine maximale Zuverlässigkeit des Netzwerk- und Produktionssystems. Diese Funktion kann beispielsweise auch verwendet werden, um vorhandene Netzwerke zu erweitern, während sie in Betrieb sind.

NxS-Switches verfügen auch über einen SNMP-Verwaltungsagenten und eine integrierte webbasierte Verwaltung. Diese Merkmale sorgen für einfache, leicht zu handhabende Konfigurationsfunktionen und damit für eine schnelle Installation und Einstellung. Auch tragen umfangreiche Netzwerk- und Geräteinformationen zu einer maximalen Systemzuverlässigkeit bei.

NxS-Switches sind kompakte Hochleistungsgeräte für industrielle Anwendungen, die auf einer Standard-DIN-Schiene installiert werden können. Die Switches verfügen über fünf Twisted-Pair-Anschlüsse (10/100 Mbit/s mit automatischer Einstellung) und zwei Anschlüsse (100 Mbit/s), die als Twisted-Pair oder Multimode-Lichtwellenleiter verfügbar sind.

Die 24-V-Betriebsspannung wird über eine Anschlussklemmleiste geliefert und kann auch für Redundanz konfiguriert werden. Ein zusätzlicher Kontakt an der Klemmleiste ermöglicht das direkte Lesen von Statusmeldungen. Integrierte LED-Anzeigen ermöglichen eine schnelle Installation und Fehlerbeseitigung vor Ort.

Hardware

2

Auf einen Blick

Übersicht

Die Fast-Ethernet-Switch-Baureihe ConneXium NxS besteht aus zwei Geräten. Diese Geräte können verwaltet werden und haben die gleichen Funktionen. Sie werden durch ihre Schnittstellen zum Anschließen von Segmenten unterschieden:

- 499NESx7100 - elektrischer ConneXium-Switch
- 499NOSx7100 - optischer ConneXium-Switch

Der Einfachheit halber werden diese beiden Geräte in diesem Handbuch mit NxS bezeichnet.

Inhalt dieses Kapitels

Dieses Kapitel enthält die folgenden Themen:

Thema	Seite
ConneXium-Switch 499NESx7100	14
ConneXium-Switch 499NOSx7100	15

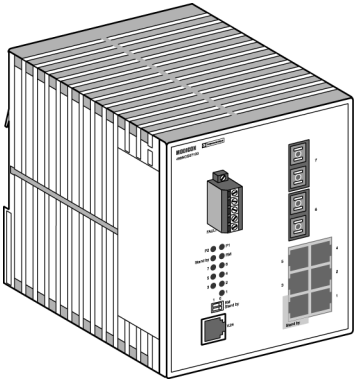
ConneXium-Switch 499NESx7100

Übersicht

Der ConneXium 499NESx7100 Dual-Speed-Switch bietet sieben Anschlüsse für geschirmte Twisted-Pair-Kabel. Dieser Switch ermöglicht das Verbinden von bis zu fünf unabhängigen SFTP-Segmenten (Shielded-and-Foiled Twisted-Pair segments, Segmente aus geschirmten und foliengeschirmten Twisted-Pair-Kabeln) mit wahlweise 10BASE-T oder 100BASE-TX und bis zu zwei unabhängigen SFTP-Segmenten mit 100 BASE-TX.

Frontansicht des 499NES17100

Die folgende Abbildung zeigt die Vorderansicht des 499NES17100.



Grundlagen zum 499NES17100

Der 499NESx7100 arbeitet in der Betriebsart "Speichern und Weiterleiten" (store-and-forward). Wenn ein Datenpaket empfangen wird, analysiert der 499NESx7100 die Herkunfts- und Zieladresse. Der Switch kann bis zu 2000 Adressen mit Portzuordnungen in seiner Adressentabelle speichern.
Der 499NESx7100 entspricht den Normen ISO/IEC 8802-3 (10BASE-T) und ISO/IEC 8802-3u (100BASE-TX).
Die LED zeigt den Empfang von Daten, Verbindungsstatus und Prozessorstatus an.
Im *Transparent Factory Benutzer- und Planungshandbuch* von Schneider Automation (Bestell-Nr. 490USE13300) wird detailliert beschrieben, wie ein lokales Netzwerk in Übereinstimmung mit ISO/IEC 8802-3 eingerichtet wird, und es werden Anleitungen für die Netzwerkplanung und die Installation von Ethernet-Netzwerken gegeben.

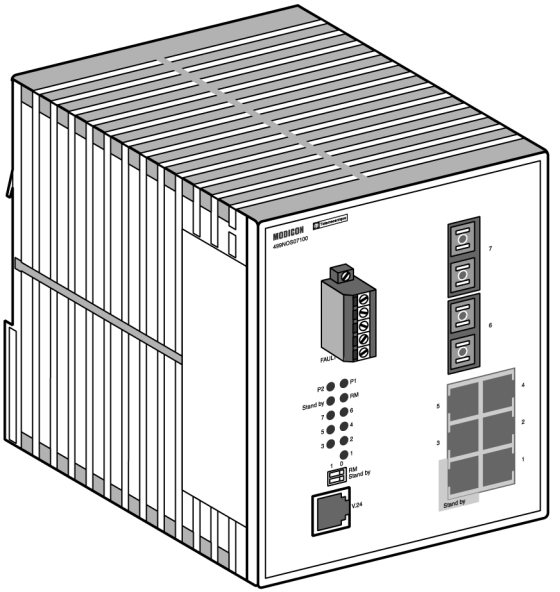
ConneXium-Switch 499NOSx7100

Beschreibung

Der Fast-Ethernet-Switch ConneXium 499NOSx7100 verfügt über fünf Anschlüsse für geschirmte Twisted-Pair-Kabel und zwei LWL-Anschlüsse. Dieser Switch ermöglicht das Verbinden von bis zu fünf unabhängigen SFTP-Segmenten (Shielded-and-Foiled Twisted-Pair segments, Segmente aus geschirmten und foliengeschirmten Twisted-Pair-Kabeln) mit wahlweise 10BASE-T oder 100BASE-TX und bis zu zwei unabhängigen LWL-Segmenten mit 100 BASE-FX.

Vorderansicht des 499NOS07100

Die folgende Abbildung zeigt die Vorderansicht des 499NOS17100.



Grundlagen des 499NOSx7100

Der 499NOSx7100 arbeitet in der Betriebsart "Speichern und Weiterleiten" (store-and-forward). Wenn ein Datenpaket empfangen wird, analysiert der 499NOSx7100 die Herkunfts- und Zieladresse. Der Switch kann bis zu 2000 Adressen mit Portzuordnungen in seiner Adressentabelle speichern.
Der 499NOSx7100 entspricht den Normen ISO/IEC 8802-3 (100BASE-FX), ISO/IEC 8802-3 (10BASE-T) und ISO/IEC 8802-3u (100BASE-TX).
Die LED zeigt den Empfang von Daten, Verbindungsstatus und Prozessorstatus an.
Im *Transparent Factory Benutzer- und Planungshandbuch* von Schneider Automation (Bestell-Nr. 490USE13300) wird detailliert beschrieben, wie ein lokales Netzwerk in Übereinstimmung mit ISO/IEC 8802-3 eingerichtet wird, und es werden Anleitungen für die Netzwerkplanung und die Installation von Ethernet-Netzwerken gegeben.

Installation und Inbetriebnahme

3

Auf einen Blick

Übersicht

Die Fast Ethernet ConneXium NxS-Schalterfamilie ist für die praktische Anwendung in einer rauhen industriellen Umgebung entwickelt worden. Dementsprechend ist der Installationsprozess einfach gehalten. In diesem Kapitel werden die wenigen Konfigurationseinstellungen beschrieben, die für den Betrieb nötig sind.

Inhalt dieses Kapitels

Dieses Kapitel enthält die folgenden Themen:

Thema	Seite
Sicherheitsinstruktionen	18
Installation von Geräten	20
Inbetriebnahme	27
Grundeinstellungen	28
TFTP-Server für Software-Aktualisierungen	39
Systemmonitor 1	44
Systemmonitor 2	48

Sicherheitsinstruktionen

Versorgungs-spannung

Die Geräte wurden für den Betrieb mit einer Sicherheits-Kleinstspannung entworfen. Darum dürfen sie entsprechend IEC950/EN60950/VDE0805 nur mit den Versorgungsspannungsanschlüssen und dem Signalkontakt mit Sicherheits-Kleinstspannung (SELV, safety extra-low voltage) verbunden werden.
Die Versorgungsspannung ist vom Gehäuse elektrisch isoliert.

WARNUNG

Mögliche Körperverletzung und/oder Materialschaden

Starten Sie nie den Betrieb mit schadhaften Komponenten!

Die Nichtbeachtung dieser Vorsichtsmaßnahmen kann den Tod, Körperverletzung oder Materialschaden zur Folge haben!

Geschirmter Erdleiter

Der geschirmte Erdleiter der anschließbaren Twisted-Pair-Leitungen ist mit der Frontplatte, die als Leiter dient, verbunden.

ACHTUNG

Mögliche Körperverletzung und/oder Materialschaden

Mögliche Kurzschlüsse sind zu vermeiden, wenn ein Kabelabschnitt mit einem leitenden Schirmgeflecht verbunden wird.

Die Nichtbeachtung dieser Vorsichtsmaßnahmen kann Körperverletzung oder Materialschaden zur Folge haben!

Gehäuse

Das Gehäuse darf nur von durch Schneider Automation autorisierten Technikern geöffnet werden.
Das Gerät ist über eine separate Erdungsschraube geerdet. Sie befindet sich links unter der Frontplatte.

- Stellen Sie sicher, dass die elektrische Installation den relevanten lokalen oder nationalen Sicherheitsbestimmungen entspricht.
- Die Lüftungsschlitze dürfen nicht bedeckt sein, damit eine freie Luftzirkulation möglich ist.
- Das Gerät darf nur in Schaltschränken mit begrenzten Energiequellen eingesetzt werden.

Umgebungs-bedingungen

Das Gerät darf nur bei einer Umgebungstemperatur von 0 bis +55 °C und einer relativen Luftfeuchtigkeit von 10 bis 90 % (nicht kondensierend) eingesetzt werden.

Qualifikations-voraussetzungen für Personal

Dieses Handbuch und die Warnungen sind für qualifiziertes Personal gedacht, das mit der Installation, Montage, Inbetriebnahme und dem Betrieb dieses Produkts vertraut und für die jeweilige Aufgabe qualifiziert sind. Dazu zählen beispielsweise Personen,

- die ausgebildet, angewiesen oder autorisiert sind, Hauptstromkreise und Geräte oder Systeme entsprechend den aktuellen technischen Sicherheitsnormen ein- und auszuschalten, zu erden und zu kennzeichnen,
- die ausgebildet oder angewiesen sind, Schutzausrüstungen entsprechend den aktuellen technischen Sicherheitsnormen zu warten und handhaben,
- die ausgebildet sind, erste Hilfe zu leisten.

Installation von Geräten

Steuerungen

Die Standby-Funktion kann mit dem 2-poligen DIP-Schalter an der Frontplatte des NxS ein- und ausgeschaltet werden.
Zustand bei Lieferung: Schalterstellung 0 (Aus), d.h. normaler Betrieb. Bei einer redundanten Kopplung mit 10/100-Mbit/s-Segmenten wird der NxS in den redundanten Abschnitten im Standby-Modus betrieben.
Die Funktion RM (Redundancy Manager, Redundanzverwaltungsprogramm) kann mit dem RM-Schalter ein- oder ausgeschaltet werden. Zustand bei Lieferung: Schalterstellung 0 (Aus), d.h. RM-Funktion nicht aktiv.

Hinweis: Aktivieren Sie nur eine der beiden Funktionen Standby und RM. Wenn beide Funktionen gleichzeitig aktiviert werden, wird das Gerät zurückgesetzt.

2-poliger DIP-Schalter

In der folgenden Abbildung wird der 2-polige DIP-Schalter gezeigt.

Redundancy Manager
Redundancy Mode

RM-Erfordernisse

Prüfen Sie die RM/Standby-Erfordernisse.

Schritt	Aktion
1	Prüfen Sie, ob die Schaltereinstellungen Ihren Erfordernissen entsprechen.

5-polige Anschluss-klemmleiste

Die Versorgungsspannung und der Fehlerkontakt werden über eine 5-polige Anschlussklemmleiste mit Schraubensicherung verbunden.

WARNUNG

SELV muss berücksichtigt werden.

Die NxS-Geräte sind für einen Betrieb mit einer Sicherheits-Kleinstspannung vorgesehen. Darum dürfen sie entsprechend IEC950/ EN60950/ VDE0805 nur mit den Versorgungsspannungsanschlüssen und dem Signalkontakt mit Sicherheits-Kleinstspannung (SELV, safety extra-low voltage) verbunden werden.

Die Nichtbeachtung dieser Vorsichtsmaßnahmen kann den Tod, Körperverletzung oder Materialschaden zur Folge haben!

Versorgungs-spannung

Die Versorgungsspannung kann redundant angeschlossen werden. Beide Eingänge sind entkoppelt. Die Belastung wird nicht verteilt. Bei einer redundanten Versorgung beliefert der Transformator nur den NxS mit der höheren Ausgangsspannung. Die Versorgungsspannung ist vom Gehäuse elektrisch isoliert.

Fehlerkontakt

Der Fehlerkontakt überwacht den korrekten Betrieb des NxS und ermöglicht so eine Ferndiagnose. Eine Unterbrechung des Kontakts wird über den Nullspannungsfehlerkontakt (Relaiskontakt, geschlossene Schaltung) gemeldet. Eine Unterbrechung kann verursacht werden durch:

- den Ausfall von mindestens einer der beiden Versorgungsspannungen,
- eine kontinuierliche Fehlfunktion in NxS (intern 3,3 VDC, Versorgungsspannung 1 oder 2 < 18 V, ...),
- eine defekte Verbindung von mindestes einem Port. Beim NxS kann die Anzeige des Verbindungsstatus durch die Verwaltung der einzelnen Ports maskiert werden. Im Zustand bei Lieferung wird der Verbindungsstatus nicht überwacht
- Fehler während der Selbstprüfung.

Im Standby-Modus werden die folgenden Zustände gemeldet:

- Steuerungskabel getrennt
- Steuerungskabel kurzgeschlossen
- Teilnehmergerät befindet sich im Standby-Modus

Im Normalmodus werden die folgenden Zustände gemeldet:

- Steuerungskabel kurzgeschlossen
- Teilnehmergerät befindet sich im Normalmodus

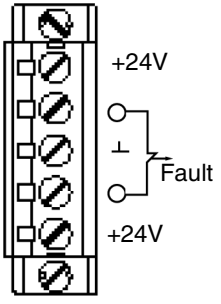
Die folgenden Zustände werden im RM-Modus gemeldet:

- Ringüberwachung ist nicht möglich, beispielsweise während der Software-Initialisierung.

Hinweis: Bei einer nicht redundanten Hauptspannungsversorgung meldet der NxS einen Stromausfall. Das Anzeigen dieser Meldung kann verhindert werden, indem die Versorgungsspannung über die beiden Eingänge angelegt wird.

Stiftbelegungen

Die folgenden Abbildung zeigt die Stiftbelegung der 5-poligen Anschlussklemmleiste



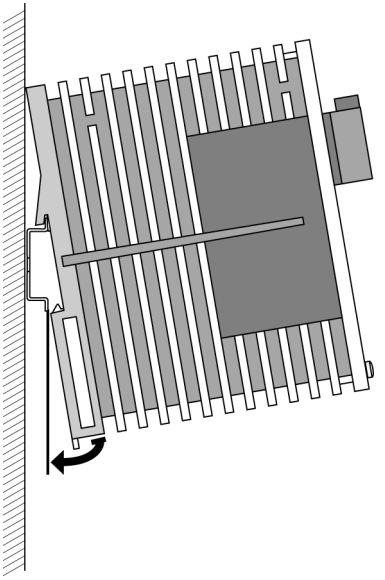
Verbinden der Leitungen

Verbinden Sie die Stromversorgung und die Signalleitungen.

Schritt	Aktion
1	Trennen Sie die Anschlussklemmleiste vom NxS, und verbinden Sie die Stromversorgung und die Signalleitungen.

Montage

Bei der Auslieferung ist das Gerät betriebsbereit.
Schieben Sie die obere Einschnappführung des NxS in die obere Hutschiene, und drücken Sie die Führung nach unten gegen die Schiene, bis sie einrastet.



Hinweis: Die Frontplatte des NxS-Gehäuses ist über eine Erdverbindung geerdet.

Hinweis: Das Gehäuse darf nicht geöffnet werden.

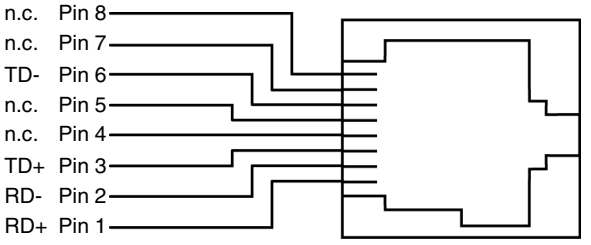
Hinweis: Der geschirmte Erdleiter der anschließbaren Twisted-Pair-Leitungen ist mit der Frontplatte, die als Leiter dient, verbunden.

10/100-Mbit/s-Verbindung

Fünf 10/100-Mbit-Ports (Port 1 bis 5, 8-polige RJ45-Buchsen) ermöglichen den Anschluss des NxS an Endgeräte oder fünf unabhängige Netzwerksegmente entsprechend den Normen ISO/IEC 8802-3 (10BASE-T) und ISO/IEC 8802-3u (100BASE-TX). Die Ports unterstützen die Funktionen "automatische Einstellung" und "automatische Polarität".
Zustand bei Lieferung: Die automatische Einstellung ist für die Ports 1 bis 5 aktiviert. Das Gerätegehäuse ist mit der Frontplatte elektrisch verbunden. Die Stiftbelegung entspricht MDI-X.
Port 1 dient zur Verbindung mit redundanten Ringen.

Stiftbelegungen

Die folgende Abbildung zeigt die Stiftbelegung einer TP/TX-Schnittstelle.



100-Mbit/s-Verbindung (Port der Hauptleitung)

Die beiden 100-Mbit/s-Ports (Port 6 und 7) ermöglichen das Einrichten einer Hauptleitung (Backbone).

- 499NESx7100: zwei Ports in Übereinstimmung mit 10/100BASE-TX (RJ45-Buchsen)
- 499NOSx7100: zwei Ports in Übereinstimmung mit 100BASE-FX (SC-Buchsen, Multimode)

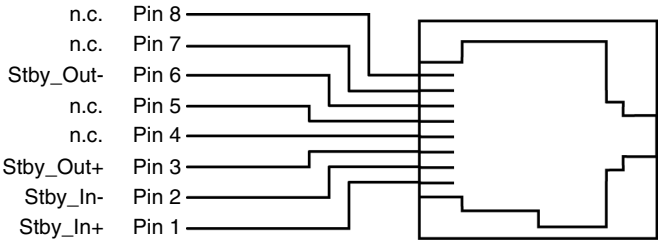
Lieferzustand: Die Ports der Hauptleitung sind auf 100 Mbit/s im Duplexbetrieb vorkonfiguriert. Diese Konfiguration wird zum Einrichten redundanter Strukturen benötigt.
Die Ports der Hauptleitung unterstützen den Duplex- und Halbduplexbetrieb. Die TX-Ports unterstützen außerdem die Funktionen automatische Einstellung und automatische Polarität.

Standby-Port

Das Steuerungskabel ist über eine 8-polige RJ45-Buchse (Standby) für den redundanten Betriebsmodus zum redundanten Koppeln von Ringen verbunden (siehe *Redundante Ringstruktur, S. 56*). Das Buchsengehäuse ist mit der Frontplatte des NxS elektrisch verbunden. Die Ausgänge Stby_Out+ und Stby_Out- sind von der Versorgungsspannung und dem Chassis (Relaiskontakt) elektrisch isoliert.

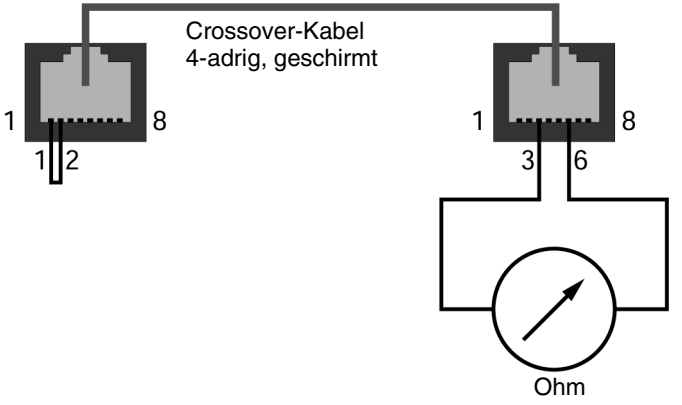
Stiftbelegung

Die folgende Abbildung zeigt die Stiftbelegung der Standby-Schnittstelle.



Länge des Steuerungskabels

Um die maximale Länge des Steuerungskabels zu bestimmen, messen Sie den Leitungswiderstand leitungsaufwärts und -abwärts. Der Gleichstromwiderstand darf 10 Ω nicht überschreiten.
Die folgende Abbildung zeigt die maximale Länge des Steuerungskabels.



V.24-Verbindung (externe Verwaltung)

Eine serielle Schnittstelle ist an der RJ11-Buchse (V.24-Schnittstelle) für die lokale Verbindung einer externen Verwaltungsstation vorhanden (VT100-Terminal oder PC mit entsprechender Terminalemulation). Dadurch wird ermöglicht, eine Verbindung mit der Benutzerschnittstelle (UI) einzurichten.
Einstellungen für VT100-Terminal:

Geschwindigkeit:	19.200 Baud (NxS07100) 9.600 Baud (NxS07100)
Daten:	8 Bit
Stopbit:	1 Bit
Quittierungsaustausch:	aus
Parität:	keine

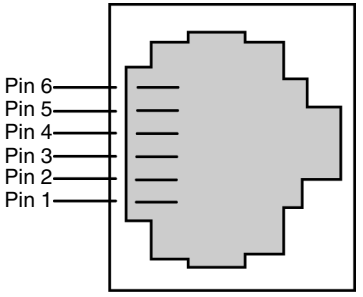
Die V.24-Verbindung kann mit den Baudraten 9600 und 19200 aktiviert werden. Die Einstellung beim Systemstart ist 19200 Baud. Das Xon/Xoff-Protokoll wird verwendet.
Das Buchsengehäuse ist mit der Frontplatte des Geräts elektrisch verbunden.
Die Signalleitungen sind von der Versorgungsspannung (60-V-Isolationsspannung) und der Frontplatte elektrisch isoliert.

Hinweis: Der NxS07100 unterstützt die Baudraten 38400 und 57600.

Hinweis: Wenn eine Verbindung eingerichtet worden ist, können Daten nicht über die Konsole übertragen werden, solange Telnet die Benutzerschnittstelle belegt. Durch Eingabe des Beendigungsbefehls über die Telnet-Verbindung wird die Benutzerschnittstelle freigegeben.

Stiftbelegung

Die folgende Abbildung zeigt die Stiftbelegung einer V.24-Schnittstelle.



Pin Number	V.24 Interface
Pin 1	CTS
Pin 2	not connected
Pin 3	TX
Pin 4	GND
Pin 5	RX
Pin 6	RTS

CTS	Clear to Send
RTS	Request to Send
RX	Receive Data
TX	Transmit Data

Leitungs-installation

Installieren der Leitungen.

Schritt	Aktion
1	Installieren Sie die Signalleitungen und erforderlichenfalls die Steuerungsleitung und das Anschlusskabel.
2	Befestigen Sie das Erdungskabel an der Erdungsschraube.

Demontage

Die folgenden Tabelle zeigt das Entfernen des NxS aus der Hutschiene.

Schritt	Aktion
1	Führen Sie den Schraubenzieher waagerecht unter das Chassis und in das Verriegelungselement ein.
2	Ziehen sie dieses nach unten - ohne den Schraubenzieher schräg zu stellen.
3	Klappen Sie den NxS auf.

Inbetriebnahme

Starten des NxS

Starten Sie den NxS, wenn die Versorgungsspannung über den 5-poligen Anschluss verbunden ist.

Schritt	Aktion
1	Starten Sie den NxS.
2	Sichern Sie die Anschlussklemmleiste mit der Feststellschraube.

Grundeinstellungen

NxS-Einstellungen

Obwohl der NxS für einfache Bedienung entworfen wurde und so weit als möglich dem "plug and play"-Prinzip entspricht, sind trotzdem einige Einstellungen erforderlich, damit die Verwaltung korrekt funktionieren kann. Um die Netzwerkverwaltung zu aktivieren, müssen Sie bei der ersten Installation des NxS eine oder mehrere IP-Adressen eingeben.
Der NxS bietet 3 Möglichkeiten zur Konfiguration von IP-Adressen:

- Konfiguration über BOOTP,
- Konfiguration über DHCP und
- Eingabe über eine V.24-Verbindung.

BOOTP (BOOTstrap-Protokoll)

Während der Inbetriebnahme empfängt der NxS seine Konfigurationsdaten entsprechend dem Ablaufdiagramm "BOOTP-Prozess" (Siehe folgende Abbildung "BOOTP/DHCP-Prozess").
Ein BOOTP-Server sollte die folgenden Daten für den NxS bereitstellen:

```
# /etc/bootptab für BOOTP-Hintergrundroutine bootpd
#
# gw -- Gateways
# ha -- Hardware-Adresse
# ht -- Hardware-Typ
# ip -- IP-Adresse
# sm -- Subnet-Maske
# tc -- Template
```

BOOTP aktivieren/ deaktivieren

Informationen zum Aktivieren/Deaktivieren von BOOTP finden Sie unter *IP-Konfiguration, S. 110* und *System, S. 70*.

DHCP-Protokoll

DHCP (Dynamic Host Configuration Protocol, dynamisches Host-Konfigurationsprotokoll) reagiert in gleicher Weise wie BOOTP und ermöglicht außerdem die Konfiguration eines DHCP-Clients mit einem Namen anstelle der MAC-Adresse. Beim DHCP-Protokoll wird dieser Name als "Client-Bezeichner" entsprechend RFC 2131 verwendet.

Der NxS verwendet den unter `sysName` eingegebenen Namen als Client-Bezeichner in der Systemgruppe von MIB II (siehe *Systemgruppe (1.3.6.1.2.1.1), S. 83*). Sie können den Systemnamen direkt über SNMP, das webbasierte Verwaltungsprogramm (siehe *System, S. 70*) oder die Benutzeroberfläche (siehe *Systemparameter, S. 109*) eingeben.

Während der Inbetriebnahme empfängt der NxS seine Konfigurationsdaten entsprechend dem Ablaufdiagramm "BOOTP/DHCP-Prozess" (siehe folgende Abbildung "BOOTP/DHCP-Prozess").

Der NxS sendet seinen Systemnamen an den DHCP-Server. Der DHCP-Server kann dann eine IP-Adresse als Alternative zur MAC-Adresse zuweisen, indem der Systemname verwendet wird.

Zusätzlich zur IP-Adresse sendet der DHCP-Server Folgendes:

- den Namen des TFTP-Servers (falls vorhanden),
- den Namen der Konfigurationsdatei (falls vorhanden).

Der NxS übernimmt diese Daten als Konfigurationsparameter (siehe *Erforderliche Schritte beim Konfigurieren des Netzwerks, S. 74*). Wenn eine IP-Adresse durch einen DHCP-Server zugewiesen wurde, wird sie dauerhaft lokal gespeichert.

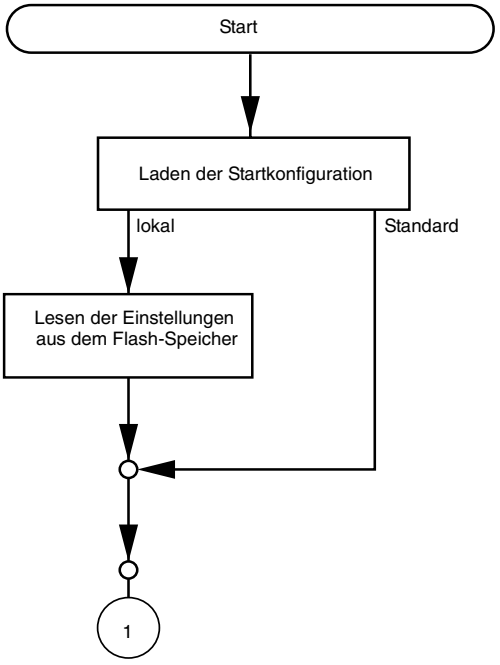
Das besondere Merkmal von DHCP im Vergleich zu BOOTP ist, dass der Server die Konfigurationsdaten nur über eine bestimmte Zeitdauer ("Überlassungsdauer") bereitstellen kann. Wenn die Zeitdauer ("Überlassungsdauer") verstrichen ist, muss der DHCP-Client versuchen, die Überlassungsdauer zu erneuern oder neu zu vereinbaren. Eine Antwort, die BOOTP ähnlich ist, kann für den Server festgelegt werden (d.h. die gleiche IP-Adresse wird immer einem bestimmten Client zugewiesen, indem die MAC-Adresse verwendet wird). Dies erfordert jedoch die explizite Konfiguration eines DHCP-Servers im Netzwerk. Wenn diese Konfiguration nicht ausgeführt wurde, wird eine gerade verfügbare Zufalls-IP-Adresse zugewiesen.

Solange DHCP aktiviert ist, versucht der NxS eine IP-Adresse zu erhalten. Wenn der NxS nach dem Neustart keinen DHCP-Server finden kann, verfügt der NxS über keine IP-Adresse.

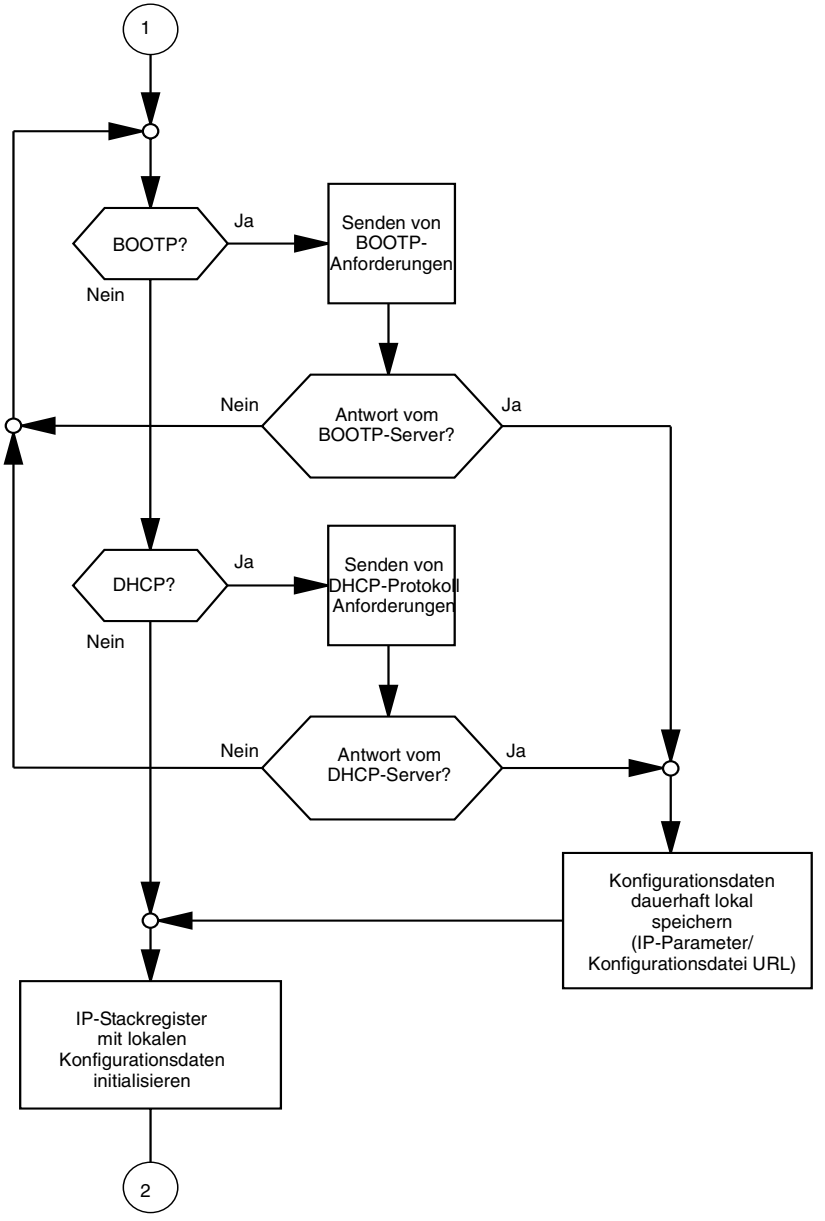
Informationen zum Aktivieren/Deaktivieren von DHCP finden Sie unter *Erforderliche Schritte beim Konfigurieren des Netzwerks, S. 74*.

BOOTP/DHCP-Prozess

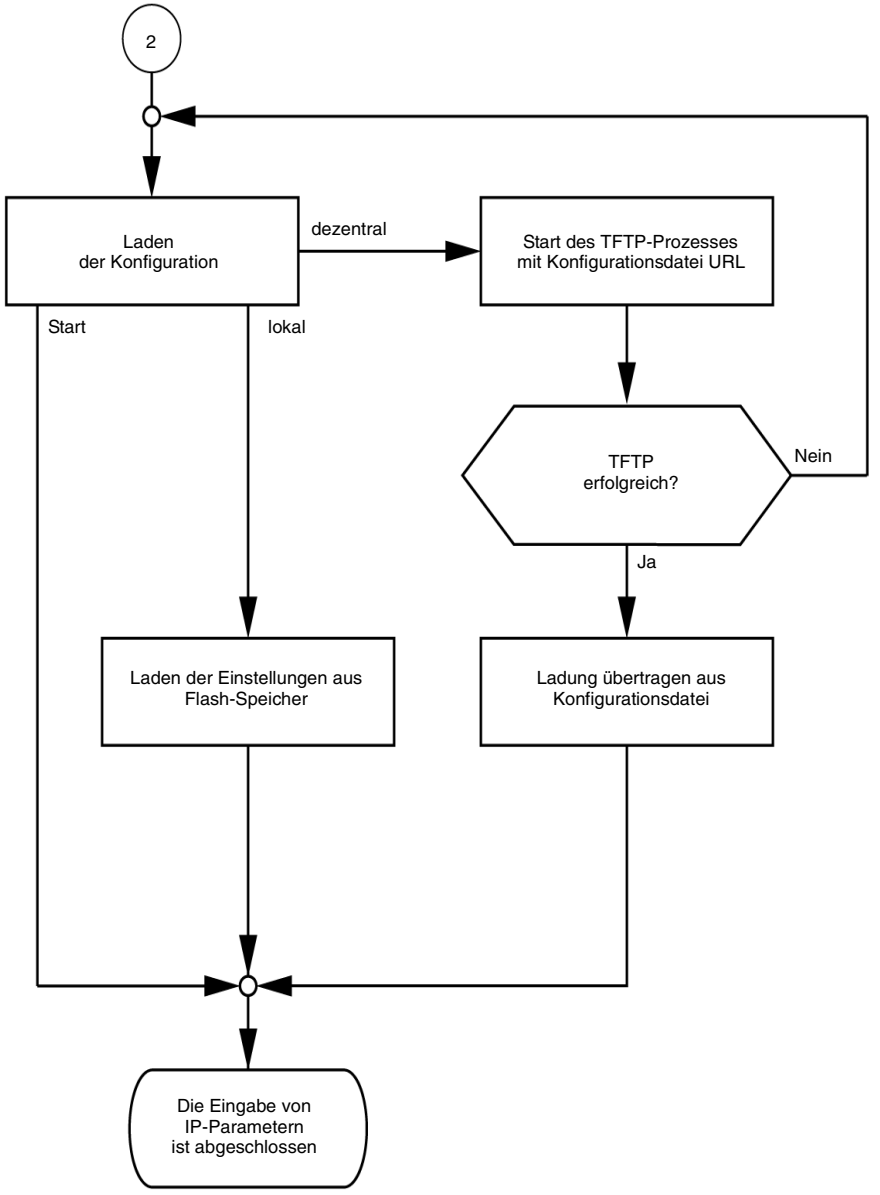
Das folgenden Ablaufdiagramm beschreibt Teil 1 des BOOTP/DHCP-Prozesses.



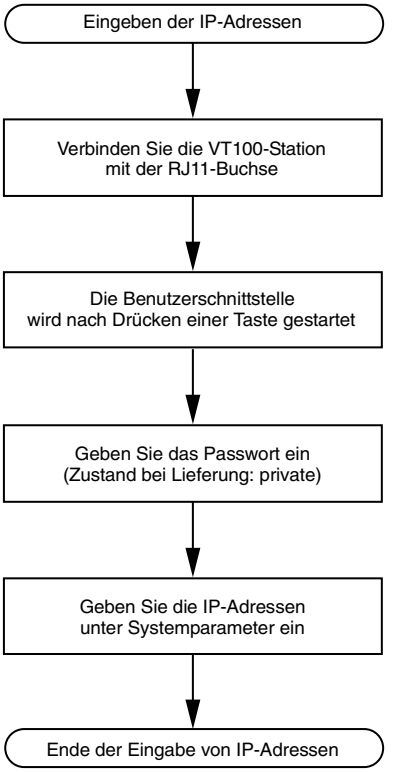
Im folgenden Ablaufdiagramm wird Teil 2 des BOOTP/DHCP-Prozesses dargestellt.



Im folgenden Ablaufdiagramm wird Teil 3 des BOOTP/DHCP-Prozesses dargestellt.



V. 24 Die folgende Abbildung beschreibt die Eingabefolge für IP-Adressen.


Eingeben der IP-Adressen
Verbinden Sie die VT100-Station mit der RJ11-Buchse
Die Benutzerschnittstelle wird nach Drücken einer Taste gestartet
Geben Sie das Passwort ein (Zustand bei Lieferung: private)
Geben Sie die IP-Adressen unter Systemparameter ein
Ende der Eingabe von IP-Adressen

Wenn keine VT100-Station in der Nähe des Installationsorts vorhanden ist, kann die IP-Adresse vor der abschließenden Installation eingegeben werden. Zu diesem Zweck wird eine VT100-Station oder eine geeignete Emulation (z.B. MS Windows-Station) benötigt.

Eingabe der IP-Adresse über eine Station

Hinweis: Die Installation des NxS ist einfacher, wenn die entsprechenden IP-Adressen für jeden NxS an Ihrer Arbeitsstation eingegeben werden. Auch wenn nur ein NxS zu installieren ist, ist es unter Umständen bequemer, die IP-Adressen an Ihrer eigenen Arbeitsstation einzugeben.

Der NxS sollte mit einer Bezeichnung versehen werden, um bei der folgenden Installation die Übersicht zu wahren.
Die Adressen werden in einem nicht flüchtigen Speicher gespeichert.
Schließen Sie eine VT100-Station oder einen PC mit Stationsemulation an die RJ11-Buchse (V.24) an.
Datenübertragungsparameter.

Geschwindigkeit:	19.200 Baud (NxS07100) 9.600 Baud (NxS07100)
Daten:	8 Bit
Parität:	keine
Stopbit:	1 Bit
Quittierungsaustausch:	aus

System-konfiguration

Nach der Installation sind folgende Schritte auszuführen.

Schritt	Aktion
1	Sobald der NxS installiert ist, starten Sie ihn, indem Sie die Stromversorgung zuschalten. Das Betriebssystem wird nach dem Drücken einer Taste geladen (siehe *Übersicht, S. 100*).
2	Geben Sie das von Ihnen zugewiesene Passwort ein (dabei ist zwischen Groß- und Kleinschreibung zu unterscheiden), und drücken Sie dann die Eingabetaste. Die Werksvorgabe für das Passwort ist: private.
3	Geben Sie die IP-Adressen ein (siehe *Systemparameter, S. 102*), und beachten Sie dabei die folgenden Erläuterungen.

Lokale IP-Adresse

Die Werksvorgabe der lokalen IP-Adresse ist: 0.0.0.0.

Gateway-IP-Adresse

Dieser Eintrag wird nur benötigt, wenn der NxS und die Verwaltungsstation bzw. der TFTP-Server sich in verschiedenen Teilnetzen befinden (siehe *Netzwerkmaske, S. 35*). Geben Sie die IP-Adresse des Gateways zwischen dem Teilnetz mit dem NxS und dem Pfad zur Verwaltungsstation ein. Die Werksvorgabe der lokalen IP-Adresse ist: 0.0.0.0.

Netzwerkmaske

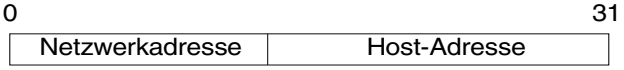
Wenn Ihr Netzwerk in Teilnetze aufgeteilt ist und diese durch eine Netzwerkmaske identifiziert werden, ist dies hier einzutragen. Die ab Werk eingetragene Masken-Adresse ist 0.0.0.0.

IP-Adresse

Die IP-Adressen bestehen aus 4 Bytes. Diese 4 Bytes werden in Dezimalschreibweise dargestellt, und jedes Byte ist durch einen Punkt getrennt. Seit 1992 gibt es fünf Klassen von IP-Adressen, die in RFC 1340 definiert sind. Die am häufigsten verwendeten Klassen sind A, B und C.
Die folgende Tabelle zeigt die Klassifizierung von IP-Adressen.

Klasse	Netzadresse	Host-Adresse
A	1 Byte	3 Bytes
B	2 Bytes	2 Bytes
C	3 Bytes	1 Byte

Die Netzwerkadresse ist der feste Teil der IP-Adresse. Sie ist vom DoD (Department of Defense) Network Information Center (Netzinformationszentrum des US-Verteidigungsministeriums) zugewiesen.
Die folgende Abbildung zeigt die Bit-Notierung bei IP-Adressen



Alle IP-Adressen gehören zur Klasse A, wenn ihr erstes Bit eine Null ist, d.h. die erste Dezimalzahl ist kleiner als 128.
Die IP-Adresse gehört zur Klasse B, wenn das erste Bit eine Eins und das zweite Bit eine Null ist, d.h. die erste Dezimalzahl liegt zwischen 128 und 191.
Die IP-Adresse gehört zur Klasse C, wenn die ersten beiden Bits eine Eins sind, d.h. die erste Dezimalzahl ist größer als 191.
Für die Zuweisung der Host-Adresse (Host-ID) ist der Netzwerkbetreiber verantwortlich. Nur der Netzwerkbetreiber ist für die eindeutige Zuweisung der von ihm zugewiesenen IP-Adressen zuständig.

Netzwerkmaske

Router und Gateways teilen große Netzwerke in Teilnetze auf. Durch die Netzwerkmaske werden die einzelnen Geräte bestimmten Teilnetzen zugewiesen. Die Unterteilung des Netzwerks in Teilnetze erfolgt in ähnlicher Weise wie die Aufteilung der IP-Adressen in die Klassen A bis C (Netz-ID).
Die Bits der Host-Adresse (Host-ID), die durch die Maske angezeigt werden sollen, werden auf Eins gesetzt. Die anderen Bits der Host-Adresse werden in der Netzwerkmaske auf Null gesetzt (siehe folgendes Beispiel).
Die folgende Abbildung zeigt ein Beispiel für eine Netzwerkmaske.

Dezimaldarstellung
255.255.192.0

Binärdarstellung
11111111.11111111.11000000.00000000

Bits der Teilnetzmaske
Klasse B

Die folgende Abbildung zeigt ein Beispiel für IP-Adressen mit Teilnetz-Zuweisung entsprechend der Netzwerkmaske aus dem vorhergehenden Beispiel.

Dezimaldarstellung
129.218.65.17

128 < 129 ≤ 191 → Klasse B

Binärdarstellung
10000001.11011010.01000001.00010001

Teilnetz 1
Netzwerkadresse

Dezimaldarstellung
129.218.129.17

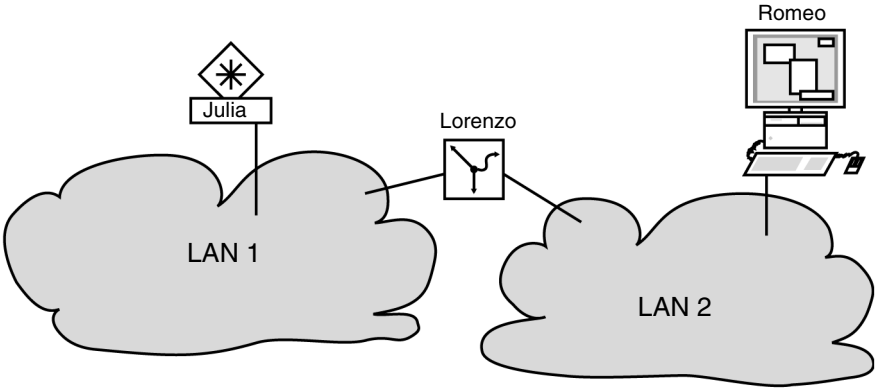
128 < 129 ≤ 191 → Klasse B

Binärdarstellung
10000001.11011010.10000001.00010001

Teilnetz 2
Netzwerkadresse

Beispiel für die Verwendung der Netzwerkmaske

In einem großen Netzwerk ist es möglich, dass Gateways und Router die Verwaltungskarte von ihrer Verwaltungsstation trennen. Wie funktioniert in solch einem Fall die Adressierung?
In der folgenden Abbildung wird ein Verwaltungsagent gezeigt, der von seiner Verwaltungsstation durch einen Router getrennt ist.



Daten senden

Die Verwaltungsstation "Romeo" möchte Daten an den Verwaltungsagenten "Julia" senden. Romeo kennt die IP-Adresse von Julia und weiss auch, dass der Router "Lorenzo" den Weg zu Julia kennt.

Beispiel

Romeo steckt seine Nachricht in einen Umschlag und beschriftet diesen mit der IP-Adresse von Julia als Zieladresse. Als Herkunftsadresse gibt Romeo seine eigene IP-Adresse auf dem Umschlag an.
Romeo steckt diesen Umschlag in einen zweiten Umschlag mit der MAC-Adresse von Lorenzo als Zieladresse und seiner eigenen MAC-Adresse als Herkunftsadresse. Dieser Prozess ist vergleichbar mit der Übertragung von Schicht 3 zur Schicht 2 des ISO/OSI-Referenzmodells.
Schließlich wirft Romeo das gesamte Datenpaket in den Briefkasten ein. Dies ist vergleichbar mit der Übertragung von Schicht 2 zu Schicht 1, d.h. mit der Übertragung des Datenpakets über das Ethernet.
Lorenzo empfängt den Brief und nimmt ihn aus dem äußeren Umschlag. Anhand des inneren Umschlags stellt er fest, dass der Brief für Julia bestimmt ist. Lorenzo steckt den inneren Umschlag in einen neuen äußeren Umschlag und sucht in seiner Adressenliste (der ARP-Tabelle) nach der MAC-Adresse von Julia. Er schreibt ihre MAC-Adresse als Zieladresse und seine eigene MAC-Adresse als Herkunftsadresse auf den äußeren Umschlag. Dann wirft er das gesamte Datenpaket in den Briefkasten ein.
Julia empfängt den Brief und nimmt ihn aus dem äußeren Umschlag heraus, wodurch die IP-Adresse von Romeo auf dem inneren Umschlag sichtbar wird. Das Öffnen und Lesen des Briefs entspricht der Übertragung der Nachricht zu den übergeordneten Protokollschichten des ISO/OSI-Schichtmodells.
Julia möchte nun eine Antwort an Romeo senden. Sie steckt ihre Antwort in einen Umschlag mit der IP-Adresse von Romeo als Zieladresse und ihrer eigenen IP-Adresse als Herkunftsadresse. Nun stellt sich die Frage, wohin Julia den Brief senden soll, da sie nicht die MAC-Adresse von Romeo erhalten hat. Die Adresse ging verloren, als Lorenzo den äußeren Umschlag ersetzte.
Julia findet in der MIB den Namen von Lorenzo unter der Variablen saNetGatewayIPAddr, die ein Mittel zum Kommunizieren mit Romeo ist. Darum steckt sie den Umschlag mit den IP-Adressen in einen weiteren Umschlag mit der MAC-Zieladresse von Lorenzo.
In gleicher Weise wie der erste Brief von Romeo an Julia gelangt der Brief nun über Lorenzo zurück zu Romeo.

TFTP-Server für Software-Aktualisierungen

Switch-Software

Die Switch-Software befindet sich im Auslieferungszustand im Flash-Speicher. Der NxS startet die Software vom Flash-Speicher aus.
Software-Aktualisierungen können über einen TFTP-Server realisiert werden. Dies setzt voraus, dass ein TFTP-Server im verbundenen Netzwerk installiert worden ist und aktiv ist.
Der NxS benötigt die folgenden Informationen, um eine Software-Aktualisierung vom TFTP-Server auszuführen:

- eine eigene IP-Adresse (dauerhaft eingetragen),
- die IP-Adresse des TFTP-Servers oder des Gateways zum TFTP-Server,
- einen Pfad für das Betriebssystem des TFTP-Servers.

Die Dateiübertragung zwischen dem NxS und dem TFTP-Server erfolgt über das TFTP-Protokoll (Trivial File Transfer Protocol).
Die Verwaltungsstation und der TFTP-Server können aus einem oder mehreren Computern bestehen.
Die Vorbereitung des TFTP-Servers für die NxS-Software beinhaltet Folgendes:

- Einrichten der NxS-Verzeichnisse und Kopieren der NxS-Software,
- Einrichten des TFTP-Prozesses.

Hinweis: Upgrades von NxS07100 zu NxS17100 sind nicht möglich.

Einrichten des TFTP-Prozesses

Dieser Abschnitt enthält Informationen zum Einrichten des TFTP-Prozesses mit einer Aufgliederung nach Betriebssystem und Anwendungen.
Allgemeine Voraussetzungen:

- Der NxS kennt die lokale IP-Adresse der NxS-IP-Adresse des TFTP-Servers/ Gateways.
- TCP/IP-Stack mit auf TFTP-Server installiertem TFTP.

SunOS und HP

In der folgenden Tabelle werden die Schritte für das Einrichten des TFTP-Prozesses aufgeführt, und die nachfolgenden Tabellen enthalten eine Aufgliederung entsprechend den Betriebssystemen und Anwendungen.

Schritt	Aktion	Kommentar
1	Prüfen Sie, ob die TFTP-Hintergrundroutine (Hintergrundprozess) läuft.	Anhand der Informationen in den nachfolgenden Tabellen können Sie bestimmen, ob der Prozess läuft.
2	Prüfen Sie, ob der Status dieses Prozesses "IW" ist.	Der Status sollte "IW" sein.
3	Prüfen Sie den TFTP-Prozess.	Informieren Sie sich anhand der folgenden Tabelle, wie der Prozess zu prüfen ist.

Prüfen des TFTP-Prozesses

Der TFTP-Prozess wird anhand der folgenden Schritte geprüft.

Schritt	Aktion

1	`cd /tftpboot/NxS`
	`tftp <TFTP-Servername>`
	`get NxS/NxS.bin`
	`rm NxS.bin`

TFTP-Installation auf HP-Workstations

Die folgende Tabelle beschreibt einen besonderen Schritt zur TFTP-Installation auf HP-Workstations.

Schritt	Aktion	Kommentar

1	Geben Sie die Benutzer-ID (tftp) in die Datei /etc/passwd ein.	Zum Beispiel:
		`tftp:*:510:20:tftp server:/usr/tftpdir:/bin/false`
		Wobei:
		`tftp = Benutzer-ID`
		`* = in das Passwortfeld`
		`510 = Muster-Benutzer-ID`
		`20 = Muster-Gruppen-ID`
		`tftp server = wählbare Bezeichnung`
		`/bin/false = obligatorischer Eintrag (Login-Shell)`

Status des SunOS-TFTP-Prozesses

Die folgende Tabelle zeigt, wie Sie bestimmen können, ob der TFTP-Prozess unter SunOS läuft.

Wenn ...	Dann ...	Kommentar
die Datei /etc/inetd.conf die Zeile `tftp dgram udp wait root /usr/etc/in.tftpd in.tftpd -s /tftpboot` enthält	läuft die TFTP-Hintergrundroutine (Hintergrundprozess).	Der Prozess muss laufen.
der Prozess nicht in der Datei enthalten ist, oder die Zeile auskommentiert ist (#)	ist /etc/inetd.conf entsprechend zu ändern und dann die INET-Hintergrundroutine neu zu initialisieren.	Informieren Sie sich anhand der folgenden Tabelle, wie die INET-Hintergrundroutine neu zu initialisieren ist.

Status des HP-TFTP-Prozesses

Die folgende Tabelle zeigt, wie Sie bestimmen können, ob der TFTP-Prozess unter HP läuft.

Wenn ...	Dann ...	Kommentar
die Datei /etc/inetd.conf die Zeile `tftp dgram udp wait root /usr/etc/in.tftpd tftpd` enthält	läuft die TFTP-Hintergrundroutine (Hintergrundprozess).	Der Prozess muss laufen.
der Prozess nicht in der Datei enthalten ist, oder die Zeile auskommentiert ist (#)	ist /etc/inetd.conf entsprechend zu ändern und dann die INET-Hintergrundroutine neu zu initialisieren.	Informieren Sie sich anhand der folgenden Tabelle, wie die INET-Hintergrundroutine neu zu initialisieren ist.

Neuinitialisieren der INET-Hintergrund-routine unter SunOS

Die folgende Tabelle zeigt das Neuinitialisieren der INET-Hintergrundroutine unter SunOS.

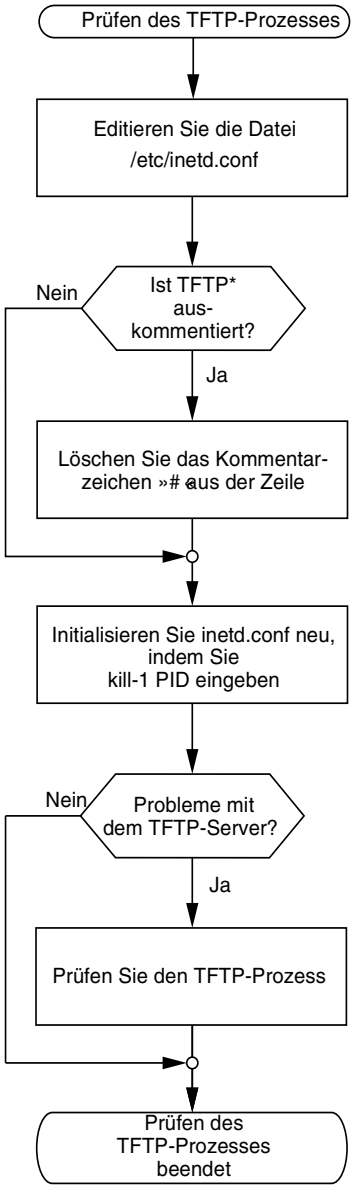
Wenn ...	Dann ...
Sie manuell neu initialisieren möchten	verwenden Sie den Befehl `kill -1 PID`, wobei PID die Prozess-ID von inetd ist.
Sie automatisch neu initialisieren möchten	verwenden Sie den Befehl `ps -ax grep inetd head -1 awk -e {print $1} kill -1`

Neuinitialisieren der INET-Hintergrund-routine unter HP

Die folgende Tabelle zeigt das Neuinitialisieren der INET-Hintergrundroutine unter HP.

Wenn ...	Dann ...
Sie manuell neu initialisieren möchten	verwenden Sie den Befehl `kill -1 PID`, wobei PID die Prozess-ID von inetd ist.
Sie automatisch neu initialisieren möchten	verwenden Sie den Befehl `/etc/inetd -c`

Ablaufdiagramm Der folgende Ablaufplan fasst die Einrichtung des TFTP-Servers unter SunOS und HP zusammen.



z.B.
cd /tftpboot/NxS
tftp <tftp-Servername>
get NxS/NxS.bin

Antwort, wenn der Prozess läuft: Empfangen ...

rm NxS.bin

* tftp dgram udp wait root/usr/etc/in.tftpd in.tftpd /tftpboot

Verzeichnisstruktur der Software

Die folgende Tabelle zeigt die Verzeichnisstruktur des TFTP-Servers mit den festgelegten Zugriffsrechten, sobald die NxS-Software installiert wurde.

Dateiname	Zugriff
NxS.bin	444-r--r--r-

d = directory (Verzeichnis), r = read (lesen), w = write (schreiben), x = execute (ausführen)
die erste Stelle bezeichnet d (directory)
die Stellen 2 bis 4 bezeichnen die Zugriffsrechte des Benutzers
die Stellen 5 bis 7 bezeichnen die Zugriffsrechte von Benutzergruppen
die Stellen 8 bis 10 bezeichnen die Zugriffsrechte aller anderen Teilnehmer.

Systemmonitor 1

Übersicht

Systemmonitore erleichtern die Aktualisierung des Betriebssystems. Die Software-Aktualisierung kann über V.24 oder TFTP ausgeführt werden. Die V.24-Schnittstelle des NxS unterstützt die Baudraten 9.600 und 19.200.

Hinweis: Die V.24-Schnittstelle unterstützt die Baudraten 38.400 und 57.600 beim NxS07100.

Aktualisierung des Betriebssystems

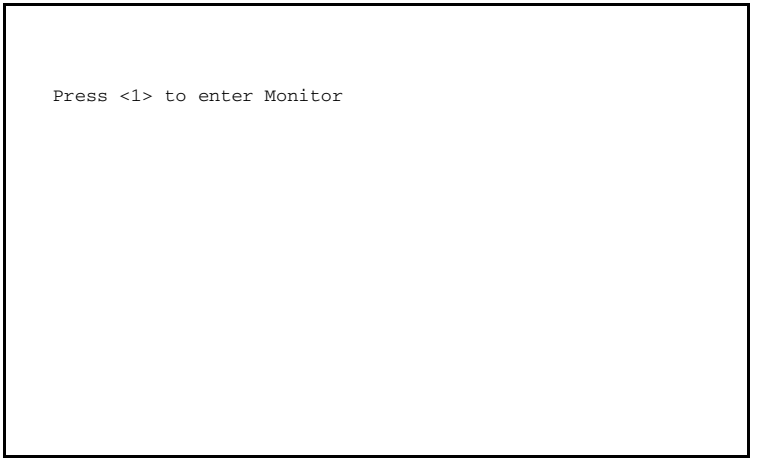
Der Systemmonitor 1 ermöglicht eine Aktualisierung des Betriebssystems des NxS über V.24.

Hinweis: Der Systemmonitor 2 wird für die Aktualisierung des Betriebssystem empfohlen.

Wenn Sie den NxS mit 9.600 Baud starten, wird an der Station die Meldung "Press <1> to enter Monitor 1" (Drücken Sie 1, um Monitor 1 aufzurufen) angezeigt.

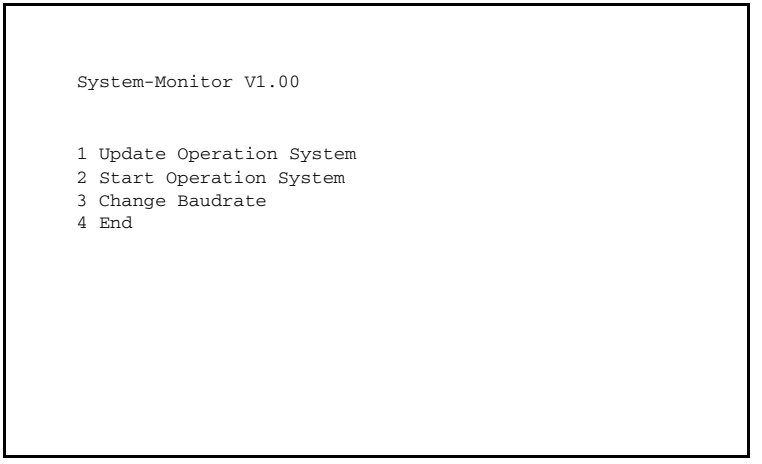
Startphase

Die folgende Abbildung zeigt die Bildschirmanzeige während der Startphase.



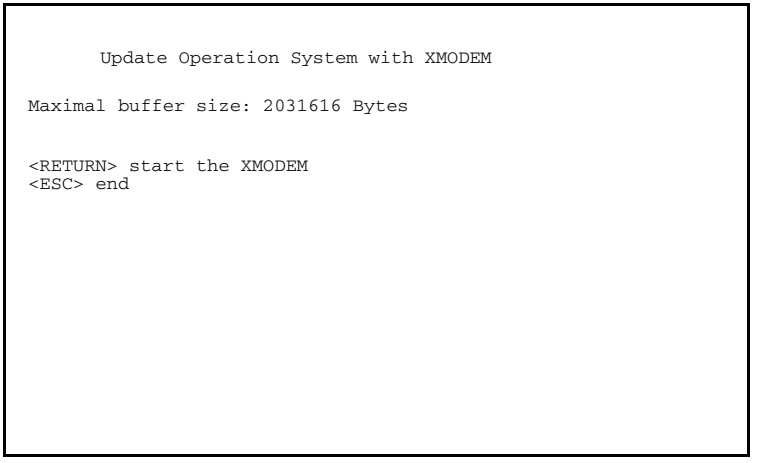
Hauptmenü des Systemmonitors 1

Drücken Sie innerhalb einer Sekunde die Taste <1>, um den Systemmonitor 1 zu starten. Der Systemmonitor 1 zeigt die folgenden Auswahlmöglichkeiten an.



Aktualisieren des Betriebssystems

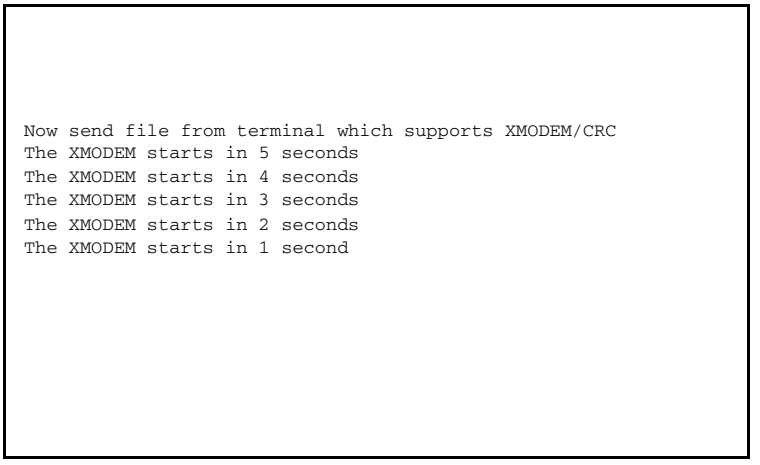
Die erste Option startet eine Aktualisierung des Betriebssystems.
Das Fenster **Update Operation System** (Betriebssystem aktualisieren) wird angezeigt.



Um zum Hauptmenü des Systemmonitors 1 zurückzukehren, drücken Sie die Taste **<ESC>**. Drücken Sie die **<EINGABETASTE>**, um die Aktualisierung mit XMODEM zu starten.

Bestätigen der Aktualisierung des Betriebssystems

Durch Drücken der **<EINGABETASTE>** wird das folgende Fenster auf dem Bildschirm angezeigt.


Now send file from terminal which supports XMODEM/CRC
The XMODEM starts in 5 seconds
The XMODEM starts in 4 seconds
The XMODEM starts in 3 seconds
The XMODEM starts in 2 seconds
The XMODEM starts in 1 second

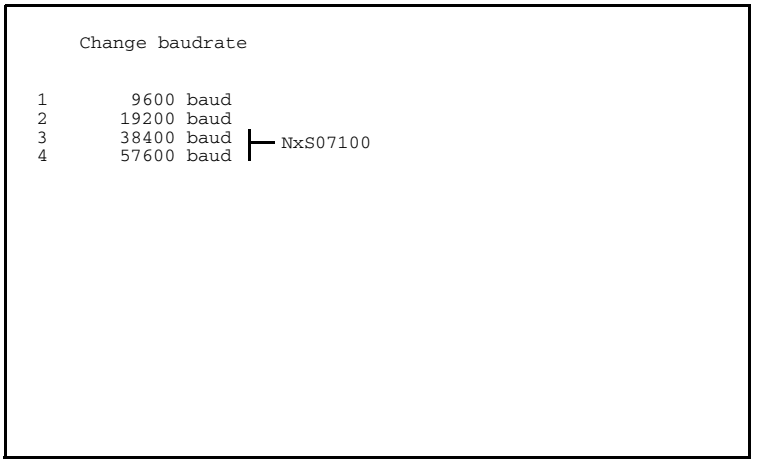
Geben Sie danach den Namen des Pfads ein, in den das Betriebssystem gespeichert werden soll. Geben Sie den Pfadnamen über das Terminalprogramm ein, beispielsweise unter Transmission Binary File (Binärdatei-Übertragung). Die Übertragung beginnt. Wenn die Übertragung beendet ist, wird das Betriebssystem neu gestartet.

Starten des Betriebssystems

Mit der zweiten Option wird das Betriebssystem gestartet.
Der Systemmonitor 1 wird beendet. Das Betriebssystem wird mit 19.200 Baud gestartet (9.600 Baud beim NxS07100).

Ändern der Baudrate

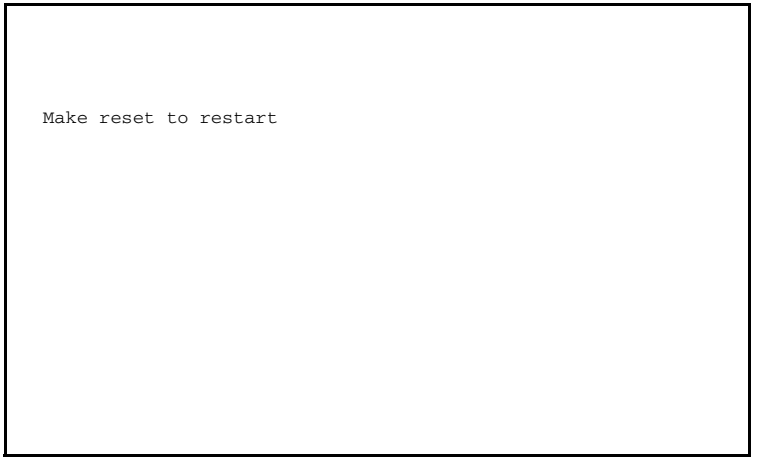
Mit der dritten Option können Sie die Baudrate ändern.
Das Fenster **Change Baudrate** (Baudrate ändern) wird angezeigt.



Zur Aktualisierung Ihres Betriebssystems (siehe Menü 1) sollten Sie die maximale Schrittgeschwindigkeit für die Baudrate wählen.
Anschließend passen Sie die Schrittgeschwindigkeit Ihres Terminalprogramms an diese Baudrate an.

Ende

Mit der vierten Option wird der Systemmonitor 1 beendet.
Das folgende Fenster wird auf dem Bildschirm angezeigt:



Danach führen Sie eine Hardware-Rücksetzung aus.

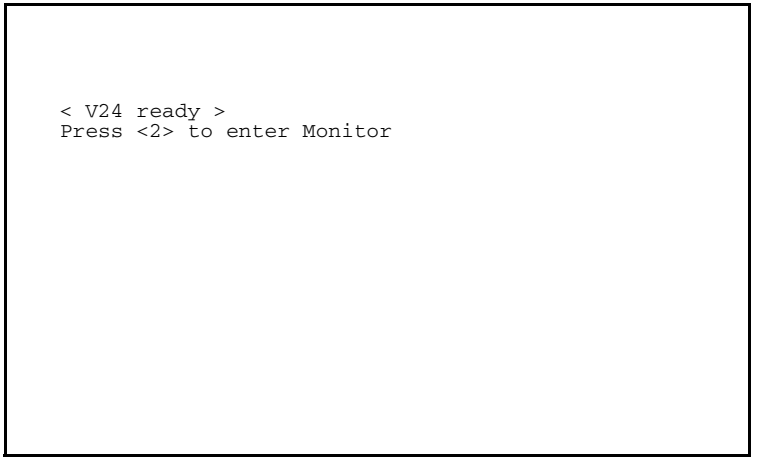
Systemmonitor 2

Übersicht

Der Systemmonitor 2 erleichtert das Aktualisieren des NxS-Betriebssystems über V.24 sowie über TFTP.

Startphase

Wenn Sie den NxS mit 9.600 Baud starten (19.200 Baud beim NxS07100), erscheint das folgende Fenster auf dem Bildschirm.



Drücken Sie innerhalb von drei Sekunden die Taste <2>, um den Systemmonitor 2 zu starten.

Hauptmenü des Systemmonitors 2

Der Systemmonitor 2 zeigt die folgenden Auswahlmöglichkeiten an.

```
System Monitor 2 V1.00

1    Software Update V24
2    Software Update TFTP
3    Cancel automatic update
4    Change Baudrate
5    Set Factory Settings
6    Reset
7    End/Quit
```

Softwareaktualisierung über V.24

Durch Auswahl der ersten Option wird eine Aktualisierung des Betriebssystems im Flash-Speicher des NxS ausgeführt. Die Aktualisierung läuft über V.24.

Hinweis: Für die Aktualisierung des Betriebssystems wird die TFTP-Übertragung empfohlen (siehe *Aktualisierung, S. 104*). Sie ist mehr als dreimal schneller als die schnellste V.24-Übertragung.

Das Fenster **Update Operation System** (Betriebssystem aktualisieren) wird angezeigt.

```
      Update Operation System with XMODEM

Maximal buffer size: 2031616 Bytes


 <RETURN> start the XMODEM
 <ESC> end
```

Um zum Hauptmenü des Systemmonitors 2 zurückzukehren, drücken Sie die Taste **<ESC>**.

Bestätigen der Aktualisierung des Betriebssystems

Durch Drücken der **<EINGABETASTE>** wird XMODEM gestartet und das folgende Fenster wird auf dem Bildschirm angezeigt.

```
Now send file from terminal which supports XMODEM/CRC
The XMODEM starts in 5 seconds
The XMODEM starts in 4 seconds
The XMODEM starts in 3 seconds
The XMODEM starts in 2 seconds
The XMODEM starts in 1 second
```

Geben Sie danach den Namen des Pfads ein, über den das Betriebssystem geladen werden soll. Geben Sie den Pfadnamen über das Terminalprogramm ein, beispielsweise unter Transmission Binary File (Binärdatei-Übertragung). Die Übertragung beginnt. Wenn die Übertragung beendet ist, wird das Betriebssystem neu gestartet.

Softwareaktualisierung über TFTP

Durch Wählen der zweiten Option wird eine Aktualisierung des Betriebssystems im Flash-Speicher des NxS ausgeführt. Die Aktualisierung läuft über TFTP.

Abbrechen der automatischen Aktualisierung

Durch Wählen der dritten Option wird die laufende automatische Softwareaktualisierung abgebrochen.

Ändern der Baudrate

Durch Auswahl der vierten Option wird die Baudrate geändert.

Zurücksetzen auf die Werkseinstellung

Durch Auswahl der fünften Option, werden die Originaleinstellungen wiederhergestellt. Mit Ausnahme der IP-Parameter werden alle SNMP-MIB-Variablen auf die Standardwerte zurückgesetzt.

Rücksetzung

Durch Auswahl der sechsten Option wird bewirkt, dass das Gerät eine Rücksetzung ausführt.

Ende/Beenden

Durch Auswahl der siebenten Option wird der Systemmonitor 2 beendet. Die Verwaltungssoftware wird gestartet.

Funktionen

4

Auf einen Blick

Übersicht

Die Geräte der Ethernet ConneXium NxS-Schalterfamilie verfügen über eine Vielzahl von Funktionen, die in diesem Kapitel vorgestellt werden.

Inhalt dieses Kapitels

Dieses Kapitel enthält die folgenden Themen:

Thema	Seite
Hardware-Funktionen	52
Anzeigen	53
Datenblockvermittlung	54
Redundanz	55
GMRP	59
Sicherheit und SNMP-Traps	61

Hardware-Funktionen

Diagnose

Beim Neustart führt der NxS eine Hardware-Selbstprüfung aus.
Während des Betriebs überwacht ein integriertes Überwachungsprogramm (Überwachungseinheit) die Funktion der Software.

Automatische Einstellung

Die automatische Einstellung ist ein Verfahren, in welchem der Switch automatisch die Betriebsart seiner 10/100-RJ45-Ports wählt. Wenn eine Verbindung zum ersten Mal eingerichtet wird, ermittelt der Switch die Übertragungsgeschwindigkeit (10 oder 100 Mbit/s) und den Übertragungsmodus des verbundenen Netzwerks (Halbduplex oder Duplex). Durch die automatische Einstellung der Ports entfällt die Notwendigkeit des manuellen Eingreifens durch den Benutzer. Die automatische Einstellung wird durch das Web-Verwaltungswerkzeug aktiviert/deaktiviert.

Automatische Polarität

Wenn das Twisted-Pair-Kabel der Empfangsleitung nicht richtig angeschlossen ist (RD+ und RD- sind vertauscht), wird die Polarität automatisch umgekehrt.

Leitungsüberwachung mit Twisted-Pair

Mit Hilfe regelmäßiger Verbindungsprüfimpulse entsprechend den Normen ISO/IEC 8802-3 (10BASE-T) und ISO/IEC 8802-3u (100BASE-TX) überwacht der NxS die verbundenen TP/TX-Leitungssegmente, um Kurzschlüsse oder Unterbrechungen zu erkennen. Der NxS sendet keine Daten an ein TP/TX-Segment, von dem er keine Verbindungsprüfimpulse empfängt.

Hinweis: Eine nicht zugewiesene Schnittstelle wird als Leitungsunterbrechung interpretiert. Die TP/TX-Leitung zu einem deaktivierten Endgerät wird auch als Leitungsunterbrechung interpretiert, da das stromlose verbundene Gerät unfähig ist, Verbindungsprüfimpulse zu senden.

Leitungsüberwachung mit Lichtwellenleitern

Ein NxS überwacht die verbundenen Lichtwellenleiter entsprechend der Norm ISO/IEC 8802-3u (100BASE-FX), um Unterbrechungen zu erkennen.

Rücksetzung

Der NxS wird durch die folgenden Ereignisse zurückgesetzt:
- Verwaltung
- nicht ausreichendes Niveau beider Eingangsspannungen
- Überwachungsprogramm

Die folgenden Aktionen werden nach einer Rücksetzung ausgeführt:
- Selbstprüfung
- Initialisierung

Anzeigen

Gerätestatus

Diese LEDs liefern Informationen über Zustände, welche den Betrieb des gesamten NxS betreffen.

LED	Leuchtet	Leuchtet nicht
P1 - Strom 1 (grün)	Versorgungsspannung 1 wird geliefert.	Versorgungsspannung 1 ist kleiner als 18 V
P1 - Strom 2 (grün)	Versorgungsspannung 2 wird geliefert.	Versorgungsspannung 2 ist kleiner als 18 V
FEHLER - Fehler (rot)	Der Signalkontakt ist offen, d.h. ein Fehler wird gemeldet.	Der Signalkontakt ist geschlossen, d.h. es wird kein Fehler gemeldet.
Standby (grün)	Die Standby-Funktion ist eingeschaltet.	Die Standby-Funktion ist ausgeschaltet.
RM - Redundanzverwaltungs-programm (grün/gelb)	**grün:** RM-Funktion aktiv, redundanter Port nicht aktiv. **gelb:** RM-Funktion aktiv, redundanter Port aktiv.	RM-Funktion nicht aktiv.

Port-Status

Diese LEDs zeigen portbezogene Informationen an.

1 bis 7 - (LED, grün/gelb)	Daten, Verbindungsstatus
Leuchtet nicht	Keine gültige Verbindung
Grün	Gültige Verbindung
Blinkt grün (einmal pro Dauer)	Port ist auf Standby geschaltet (Port 1)
Blinkt grün (dreimal pro Dauer)	Port ist deaktiviert
Blinkt gelb	Datenempfang
Blinkt fortlaufend	Initialisierungsphase nach Neustart

Datenblockvermittlung

Speichern und Weiterleiten

Sämtliche von einem NxS empfangenene Daten werden gespeichert und auf Gültigkeit überprüft. Ungültige und fehlerhafte Datenpakete (> 1522 Bytes oder CRC-Fehler, >1518 Bytes beim NxS07100) sowie Fragmente (< 64 Bytes) werden gelöscht. Gültige Datenpakete werden durch den NxS weitergeleitet.

Fähigkeit der Verwendung von Mehrfach-adressen

Ein NxS lernt alle Herkunftsadressen für einen Port. Nur Pakete mit

- unbekannten Adressen
- diesen Adressen oder
- einer Mehrfach-/Broadcast-Adresse

im Zieladressenfeld werden zu diesem Port gesendet.
Ein NxS kann bis zu 2000 Adressen lernen. Dies wird notwendig, wenn mehr als ein Endgerät mit einem oder mehreren Ports verbunden ist. Auf diese Weise ist es möglich, mehrere unabhängige Teilnetze mit einem NxS zu verbinden.

Lernen von Adressen

Ein NxS überwacht das Alter der gelernten Adressen. Adresseinträge, die ein bestimmtes Alter überschreiten (30 sek, Alterungszeit) werden durch den NxS aus seiner Adressentabelle gelöscht.

Hinweis: Durch einen Neustart werden die gelernten Adresseinträge gelöscht.

Prioritäten-setzung

Der NxS unterstützt zwei Prioritätsschlangen (Datenverkehrsklassen entsprechend IEEE 802.1D). Die empfangenen Datenpakete werden diesen Klassen zugewiesen durch

- die vordefinierte Zuweisung in den statischen Adresseinträgen,
- die Priorität des im VLAN-Tag enthaltenen Datenpakets.

Dieses Funktion verhindert, dass Datenverkehr mit hoher Priorität in verkehrs-starken Zeiten durch anderen Datenverkehr unterbrochen wird. Datenverkehr mit niedriger Priorität wird gelöscht, wenn der Speicher oder der Übertragungskanal überlastet ist.

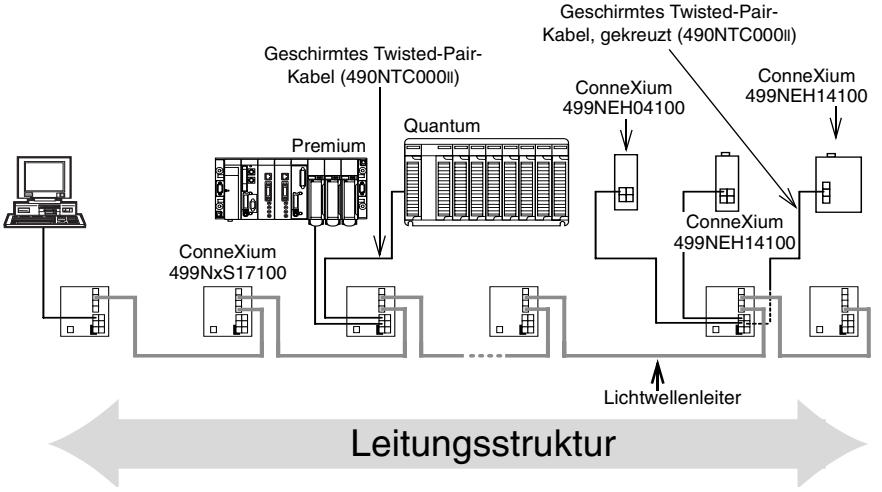
Kennzeichnung

Entsprechend der Norm IEEE 802.1 Q ist das VLAN-Tag in den MAC-Datenblock für die Funktionen VLAN und Prioritätensetzung integriert. Das VLAN-Tag besteht aus 4 Bytes. Es wird zwischen dem Herkunftsadressenfeld und dem Typ-Feld eingefügt.
Bei Datenpaketen mit VLAN-Tag bewertet der NxS das 3-Bit-Prioritätsfeld innerhalb des VLAN-Tag.
Der MAC-Datenblock wird durch den NxS unverändert übertragen.

Redundanz

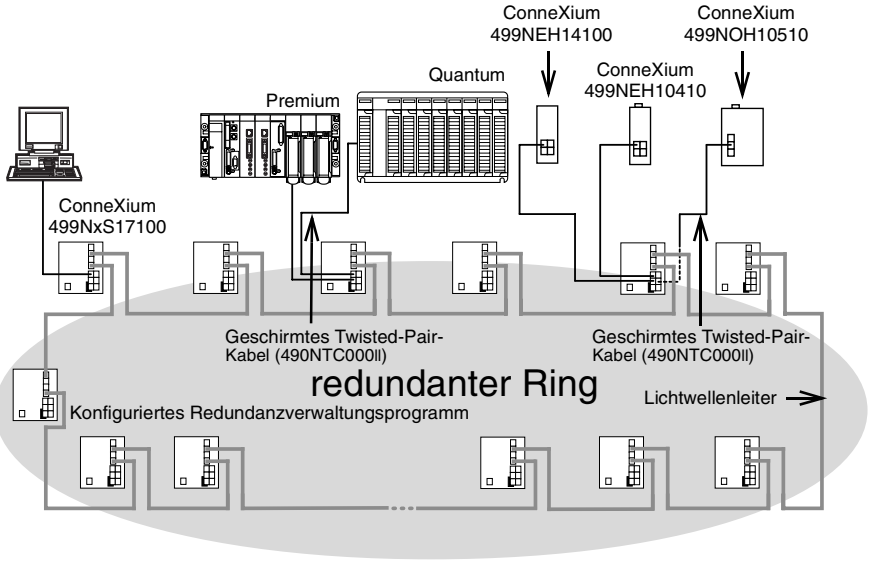
Bustyp-konfiguration

Der NxS ermöglicht die Einrichtung von Hauptleitungen (Backbones) über die Bustypkonfiguration. Das Kaskadieren erfolgt über die Hauptleitungsports.
In der folgenden Abbildung wird gezeigt, wie Hauptleitungen in einer Buskonfiguration eingerichtet werden können.



Redundante Ringstruktur

Die beiden Enden einer Hauptleitung in einer Buskonfiguration können geschlossen werden, um einen redundanten Ring zu bilden, indem die RM-Funktion (**R**edundancy **M**anager, Redundanzverwaltungsprogramm) des NxS verwendet wird.
In der folgenden Abbildung wird ein Beispiel der Struktur eines redundanten optischen Rings gezeigt.

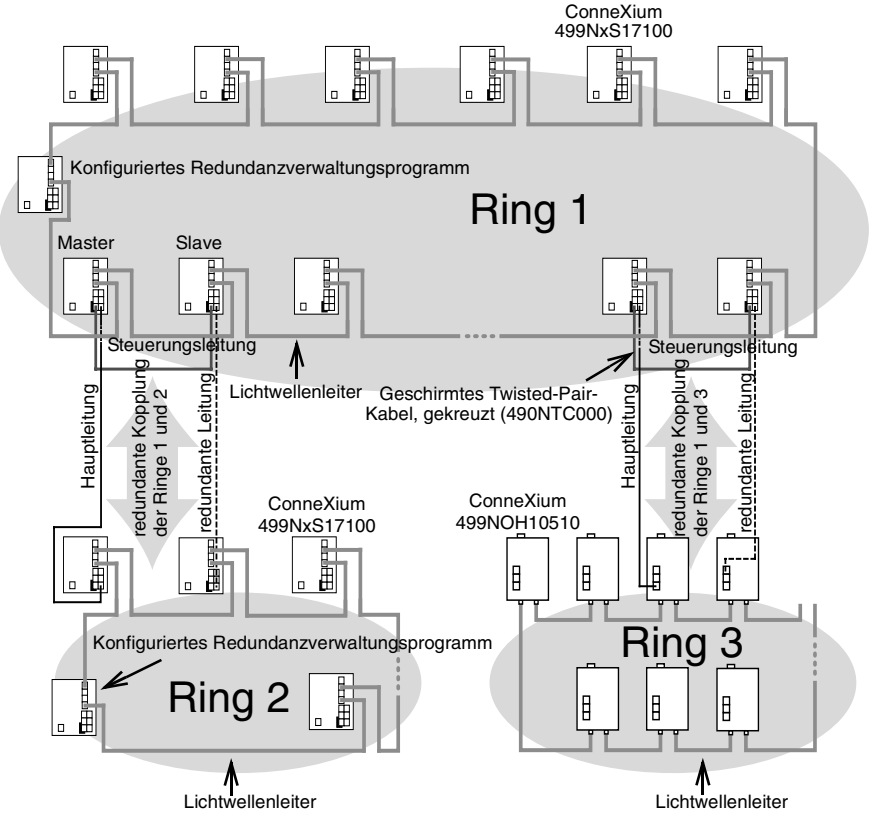


Der NxS ist über die Hauptleitungsports (Ports 6 und 7) in den Ring integriert. Wenn ein Leitungsabschnitt ausfällt, wird die Ringstruktur von bis zu 50 NxS-Switches innerhalb von 0,5 sek zurück in eine Buskonfiguration umgewandelt.

Hinweis: Die Funktion "Redundanter Ring" erfordert die folgende Einstellung für die Ports 6 und 7: 100 Mbit/s, Duplexbetrieb und automatische Einstellung (Werkseinstellung).

Redundante Kopplung von Netzwerk-segmenten

Die eingebaute Steuerungsintelligenz des NxS ermöglicht die Kopplung von Netzwerksegmenten.
In der folgenden Abbildung wird gezeigt, wie Netzwerksegmente in einer Kopplungskonfiguration redundanter Ringe verbunden werden können.



Zwei Netzwerksegmente sind über zwei separate Pfade mit jeweils einem NxS verbunden. Die Redundanzfunktion wird dem NxS in der redundanten Verbindung über die Einstellung des Standby-DIP-Schalters zugewiesen.
Der NxS in der redundanten Leitung und der NxS in der Hauptleitung informieren sich untereinander über die Steuerungsleitung (gekreuztes Twisted-Pair-Kabel) über ihre Betriebszustände.

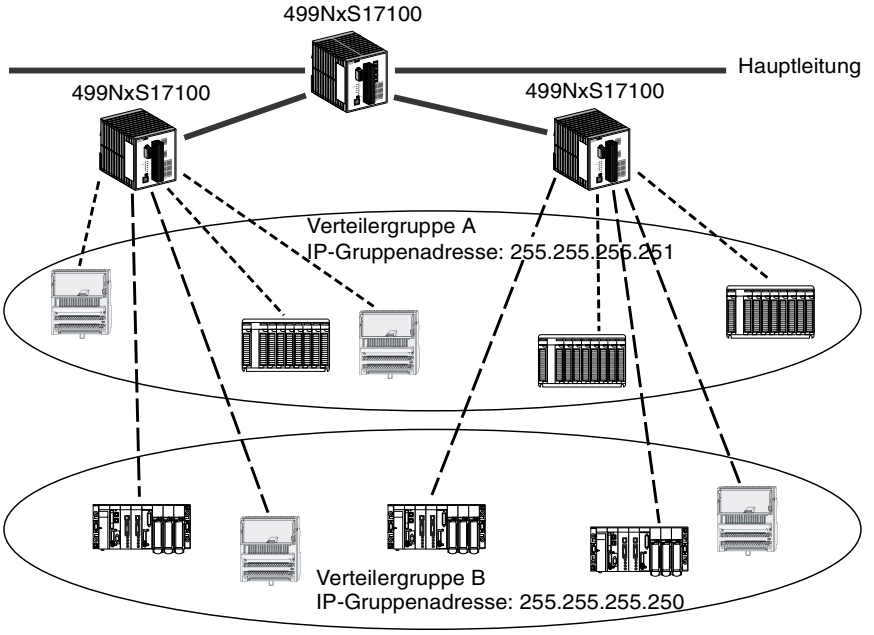
Hinweis: Die Hauptleitung und die redundanten Leitungen müssen mit Port 1 des entsprechenden NxS-Switches verbunden werden.

Unmittelbar nach dem Ausfall der Hauptleitung gibt die redundante NxS-Leitung die redundante Leitung frei. Sobald der normale Betrieb der Hauptleitung wiederhergestellt ist, informiert der NxS in der Hauptleitung den redundanten NxS. Die Hauptleitung wird freigegeben, und die redundante Leitung wird wieder blockiert. Ein Fehler wird innerhalb von 0,5 sek erkannt und beseitigt.

GMRP

Arbeiten mit GMRP in einer Automations-einstellung

Im GMRP-Protokoll (GARP Multicast Registration Protocol, GMRP) wird angegeben, wie Multicast-Sendungen an andere Switches verteilt werden. Dadurch können Switches Multicast-Adressen lernen.
In der folgenden Abbildung wird gezeigt, wie GMRP in einer Automationseinstellung verwendet wird.



GMRP ist in einer Automationseinstellung hilfreich, wenn durch Switches mehrere Gruppen von Modulen anhand des Dienstes für globale Daten verbunden werden.

Hinweis: Durch den Dienst für globale Daten werden Variablen über das Netzwerk ausgetauscht, um Automationsanwendungen zu synchronisieren.

Die ConneXium-Switches (499NxS17100, V4.0) und SAUT-Ethernet-Module (TSX ETY4102/5102, 140NOE77x1) verhindern mit Hilfe von GMRP eine Überlastung des Netzwerks, indem Daten nur an die Multicast-Adresse der lokalen Verteilergruppe gesendet werden. Die Ethernet-Module senden ihre Muticast-Adressen an die Switches. Die Switches lernen die Adressen und leiten dann Multicast-Sendungen nur an die Ports weiter, die Mitglieder der gleichen Gruppe sind.

Die Baumstruktur für Multicast-Sendungen wird innerhalb von 5 Sekunden in einem Netzwerk mit bis zu 20 NsX-Modulen eingerichtet, nachdem die Gruppenadresse erstmalig am NxS-Port eingegeben wurde.
Geräte, die GMRP nicht unterstützen, können durch einen statischen Filteradressseintrag am Verbindungsport in das Multicast-Adressierungsschema integriert werden.

Aktivieren von GMRP mit SNMP

Im Lieferzustand ist GMRP bei allen Ports deaktiviert.
Multicast-Filterung kann aktiviert werden, indem einer der Switch-Parameter über SNMP (Simple Network Management Protocol) geändert wird. Gegenwärtig ist dies die einzige Möglichkeit, diesen Parameter zu ändern.
Zum Ändern dieses Parameters benötigen Sie einen SNMP-MIB-Browser oder ein SNMP-Verwaltungsprogramm.
Der Parameter kann auf zwei Arten geändert werden:

- Direkter Zugriff auf den Parameter - zum direkten Zugriff auf das Objekt kann der Benutzer den Browser anweisen, die Objekt-ID auszulesen: 1.3.6.1.2.1.17.6.1.1.3.0
- Durchsuchen der MIB-Objekte im Gerät - zum Durchsuchen der Objekte muss der Benutzer die folgenden MIBs erhalten und in den Browser installieren:
  - Definitions of Managed Objects for Bridges, RFC 1493 (Definitionen für verwaltete Objekte für Bridges)
  - Definitions of Managed Objects for Bridges with Traffic Classes, Multicast Filtering and Virtual LAN Extensions, RFC 2674 (Definitionen für verwaltete Objekte für Bridges mit Verkehrsklassen, Multicast-Filterung und virtuellen LAN-Erweiterungen)

Nach dem Zugriff auf das Objekt sollten Sie den Wert auf "1" setzen, um Multicast-Filterung zu aktivieren, oder auf "2", um Multicast-Filterung zu deaktivieren.
Eine vollständige Beschreibung des zu ändernden Objekts finden Sie weiter unten:

```
dot1dGmrpStatus OBJECT-TYPE
SYNTAX : EnabledStatus
MAX-ACCESS : read-write
STATUS : current
DESCRIPTION
```

"Der von der Verwaltung für GMRP angeforderte Administrativ-Status. Der Wert enabled(1) zeigt an, dass GMRP für dieses Gerät, in allen VLANs und für alle Ports aktiviert werden sollte, für die es nicht ausdrücklich deaktiviert wurde. Beim Wert disabled(2), wird GMRP deaktiviert, und zwar in allen VLANs sowie an allen Ports, und alle GMRP-Pakete werden transparent weitergeleitet. Dieses Objekt wirkt sich auf Maschinen im Zustand Applicant und Registrar aus. Ein Übergang von disabled(2) zu enabled(1) bewirkt eine Rücksetzung aller Maschinen im GMRP-Status an allen Ports."

```
::= { dot1dExtBase 3 }
```

Sicherheit und SNMP-Traps

Port-Sicherheit

Ein NxS schützt jeden Port gegen unberechtigten Zugriff. Die folgenden Funktionen sind zur Überwachung der einzelnen Ports verfügbar:
Zugriff: Der NxS erkennt 2 Klassen der Zugriffssteuerung.

- **Jeder:** keine Zugriffsbeschränkung.
- **Benutzer:** nur ein zugewiesener Benutzer hat Zugriff.

Unberechtigter Zugriff: Der NxS kann auf drei wählbare Arten auf den Versuch eines unberechtigten Zugriffs reagieren.

- **non:** keine Reaktion
- **trapOnly:** Nachricht durch Senden eines Traps
- **portDisable:** Nachricht durch Senden eines Traps und Deaktivieren eines Ports

Die Einstellungen für die Port-Sicherheit werden über einen SNMP-Netzwerkverwalter vorgenommen. Fahren Sie fort, indem Sie im Gerätefenster mit der rechten Maustaste auf das Agent-Symbol `Sicherheit` klicken. Im daraufhin angezeigten Agent-Fenster finden Sie die Tabelle mit den entsprechenden MIB-Variablen unter `Port-Sicherheit`.

SNMP

Der Agent kommuniziert mit der Netzverwaltungsstation über das Simple Network Management Protocol (SNMP). Darum verwendet die Netzverwaltungsstation die Netzverwaltungssoftware **F** oder die webbasierte Benutzeroberfläche. Jedes SNMP-Paket enthält die IP-Adresse des sendenden Computers und der Teilnehmergemeinschaft, unter welcher der Absender des Pakets auf die Verwaltungsinformationsbasis (MIB) des Switches zugreift.
Der Switch empfängt das SNMP-Paket und vergleicht die IP-Adresse des sendenden Computers und der Teilnehmergemeinschaft mit den Einträgen in der `saAuthCommTable` und der `saAuthHostTable` seiner MIB. Wenn die Teilnehmergemeinschaft über die entsprechende Zugriffsberechtigung verfügt und die IP-Adresse des sendenden Computers eingegeben ist, gestattet der Switch den Zugriff. Im Lieferzustand kann auf den Switch von jedem Computer aus über die Teilnehmergemeinschaft "öffentlich" (nur Lesen) und "privat" (Lesen und Schreiben) zugegriffen werden.

Verhindern unberechtigten Zugriffs auf den Switch

Durch die folgenden Schritte wird der NxS gesichert.

Schritt	Aktion	Kommentar
1	Definieren Sie eine neue Teilnehmergemeinschaft, auf die Sie von Ihrem Computer aus mit allen Berechtigungen zugreifen können.	Notieren Sie den Namen der Teilnehmergemeinschaft und des zugehörigen Index. Aus Sicherheitsgründen kann der Name der Teilnehmergemeinschaft nicht zu einem späteren Zeitpunkt gelesen werden. Behandeln Sie diese Teilnehmergemeinschaft mit Diskretion, da jeder, der die Teilnehmergemeinschaft kennt, mit der IP-Adresse Ihres Computers auf die Switch-MIB zugreifen kann.
2	Schränken Sie die Zugriffsrechte der bekannten Teilnehmergemeinschaften ein oder löschen Sie deren Einträge.	Der Zugriff auf die Tabelle des Gemeinschaftszugriffs, des Trap-Ziels und der Trap-Konfiguration erfolgt über den Gemeinschaftsindex.

SNMP-Traps

Falls während des normalen Betriebs des NxS ungewöhnliche Ereignisse auftreten, werden diese unmittelbar an die Verwaltungsstation gemeldet. Dies geschieht durch sogenannte Traps (Alarme), die das Abfrageverfahren umgehen ("Abfragen" bezieht sich auf das Abfragen von Datenstationen in regelmäßigen Intervallen). Traps ermöglichen das schnelle Reagieren auf kritische Situationen.
Es folgen Beispiele für solche Ereignisse:

- Hardware-Rücksetzung
- Ändern der Grundkonfiguration des Gerätes
- Segmentierung eines Ports

Traps können an mehrere Hosts gesendet werden, um die Zuverlässigkeit der Übertragung von Nachrichten zu erhöhen. Eine Trap-Nachricht ist ein Paket, das nicht quittiert ist.
Der Verwaltungsagent sendet Traps an diejenigen Hosts, die in der Trap-Zieltabelle eingetragen sind. Die Trap-Zieltabelle kann mit der Verwaltungsstation über SNMP konfiguriert werden.

Verzeichnis der SNMP-Traps

In der folgenden Tabelle sind alle Traps aufgelistet, die auftreten können.

Trap	Wird gesendet
authenticationFailure	wenn eine Station versucht, ohne Berechtigung auf einen Agent zuzugreifen.
coldStart	für einen Kalt- oder Warmstart während des Startprozesses nach erfolgreicher Verwaltungsinitialisierung. Der Trap coldStart wird bei jedem Startvorgang gesendet.
saPowerSupply	wenn sich der Status der Spannungsversorgung ändert.
saSignallingRelay	wenn sich der Status des Signalkontakts ändert.
saStandby	wenn sich der Betriebszustand des NxS ändert.
linkDown	wenn die Verbindung mit einem Port unterbrochen wird.
linkUp	wenn die Verbindung mit einem Port wiederhergestellt wird.
risingAlarm	wenn ein Alarmeingang den oberen Schwellenwert überschreitet.
fallingAlarm	wenn ein Alarmeingang unter den unteren Schwellenwert fällt.
saPortSecurityTrap	wenn eine MAC-Adresse am Port erkannt wird, die nicht mit den aktuellen Einstellungen von Folgendem übereinstimmt: `saPortSecPermission` und `saPorSecAction`, entweder auf `trapOnly` (2) oder `portDisable` (3) gesetzt.

Webbasierte Verwaltung

5

Auf einen Blick

Übersicht

Der NxS unterstützt die SNMP-Verwaltung und die webbasierte Verwaltung und kann auf diese Weise umfassende Diagnose- und Konfigurationsfunktionen für eine schnelle Installation und umfassende Netzwerk- und Geräteinformationen bereitstellen.
Der NxS unterstützt die TCP/IP-Protokollfamilie.
Die benutzerfreundliche webbasierte (Hypertext-) Schnittstelle ermöglicht das Verwalten des NxS von jeder beliebigen Stelle im Netzwerk aus über einen Standard-Browser wie Netscape Navigator/Communicator oder Microsoft Internet Explorer ab Version 4.x. Der Webbrowser ist ein universales Zugriffswerkzeug und kann direkt mit dem NxS über das HTTP-Protokoll kommunizieren. Die webbasierte Schnittstelle ermöglicht Ihnen, den NxS grafisch zu konfigurieren.

Inhalt dieses Kapitels

Dieses Kapitel enthält die folgenden Themen:

Thema	Seite
Starten der webbasierten Schnittstelle	66
Funktion der webbasierten Benutzeroberfläche	69

Starten der webbasierten Schnittstelle

Voraussetzungen

Um die webbasierte Schnittstelle zu öffnen, benötigen Sie einen Webbrowser (ein Programm, das Hypertext lesen kann), beispielsweise Netscape Navigator/ Communicator oder Microsoft Internet Explorer ab Version 4.x.

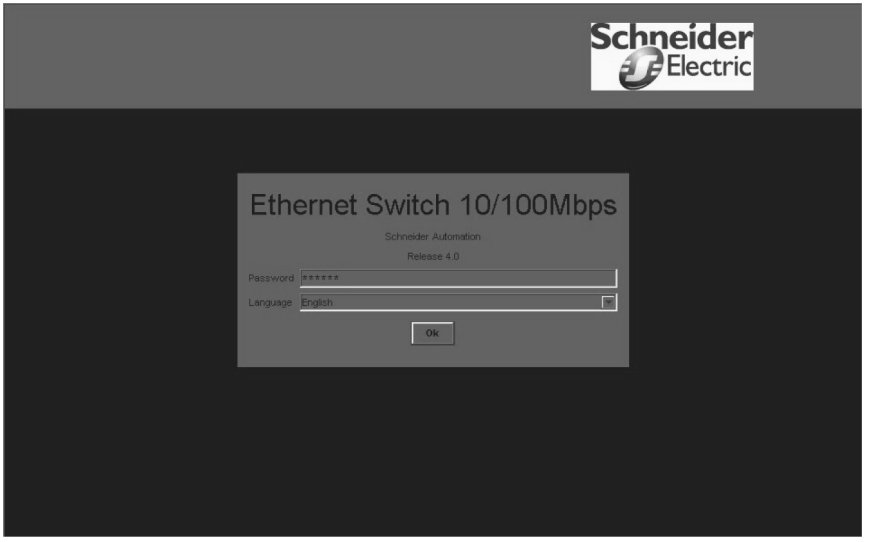
Aktivieren der webbasierten Schnittstelle

Die folgende Tabelle zeigt die Schritte zur Aktivierung der webbasierten Benutzeroberfläche.

Schritt	Aktion	Kommentar
1	Starten Sie Ihren Webbrowser.	
2	Stellen Sie sicher, dass Sie JavaScript in Ihrem Browser aktiviert haben.	
3	Stellen Sie die Verbindung her, indem Sie die IP-Adresse des NxS eingeben, mit der Sie die webbasierte Netzwerkverwaltung im Adressfeld des Webbrowsers verwalten möchten. Geben Sie die Adresse in der folgenden Form ein: `http://xxx.xxx.xxx.xxx`	Die webbasierte Benutzeroberfläche verwendet das Plugin "Java(tm) Runtime Environment Version 1.2". Falls dieses noch nicht auf Ihrem Computer installiert ist, wird es beim Starten der webbasierten Benutzerobefläche automatisch über das Internet installiert. Diese Installation ist sehr zeitaufwändig. **Für Windows NT-Benutzer:** Brechen Sie die Installation ab. Installieren Sie das Plugin von der im Lieferumfang enthaltenen CD-ROM. Fahren Sie fort, indem Sie die Programmdatei **jre1_2_1-win-i.exe** im Java-Verzeichnis auf der CD-ROM starten.

Anmelden beim NxS

Das Anmeldefenster für den NxS erscheint.

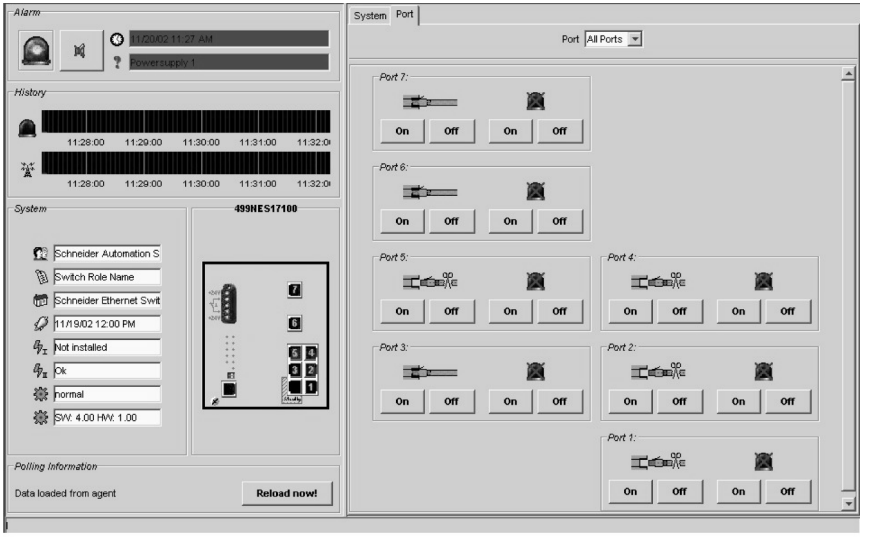


Ausführen der Anmeldung

Die folgende Tabelle enthält die Schritte zum Ausführen der NxS-Anmeldung.

Schritt	Aktion	Kommentar
1	Wählen Sie die gewünschte Sprache.	
2	Geben Sie das Passwort ein.	Das Password "public" (öffentlich) wird im Password-Feld angezeigt, mit dem eine Anmeldung mit Leseberechtigung ausgeführt werden kann. Wenn Sie mit Schreibberechtigung auf den NxS zugreifen möchten, überschreiben Sie den Inhalt des Passwort-Felds mit dem Passwort "private" (privat) (Werkseinstellung). Durch Ändern des Passworts wird der NxS gegen unberechtigten Zugriff geschützt.
3	Klicken Sie auf OK.	Die Startseite des NxS wird auf dem Bildschirm angezeigt.

NxS-Startseite Die Startseite der NxS-Website erscheint.



Funktion der webbasierten Benutzeroberfläche

NxS-Startseite

Die Seite ist in folgende Bereiche aufgeteilt:
- In einen Informationsteil (linke Seite der NxS-Startseite) und
- und einen Konfigurationsteil (rechte Seite der NxS-Startseite).

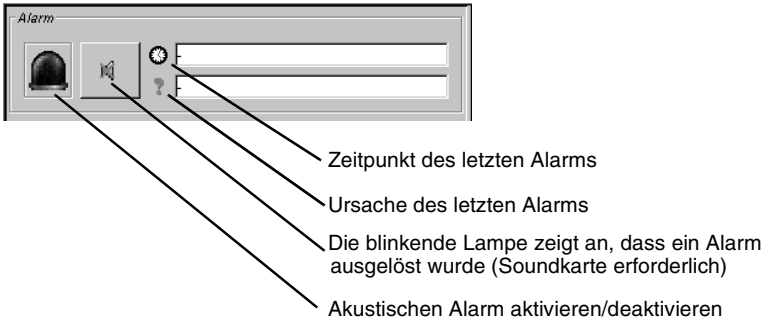
Der Konfigurationsteil (rechte Seite) besteht aus zwei Registern:
- System
- Anschluss

Informationen

Der Informationsabschnitt ist wie folgt aufgeteilt:
- Alarm
- Aufzeichnung
- System
- Ansicht des Switch
- Aktualisierung

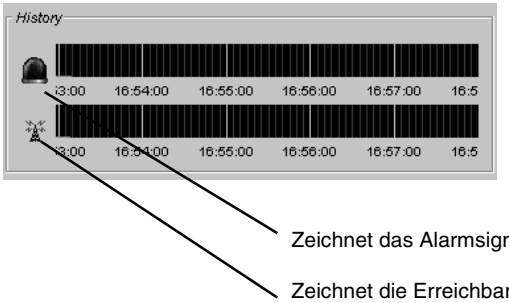
Alarm

Dieser Bereich der Startseite gibt Informationen zum Alarmzustand des NxS. Die folgende Abbildung zeigt die Komponenten der Alarmanzeige.


Alarm
Zeitpunkt des letzten Alarms
Ursache des letzten Alarms
Die blinkende Lampe zeigt an, dass ein Alarm ausgelöst wurde (Soundkarte erforderlich)
Akustischen Alarm aktivieren/deaktivieren

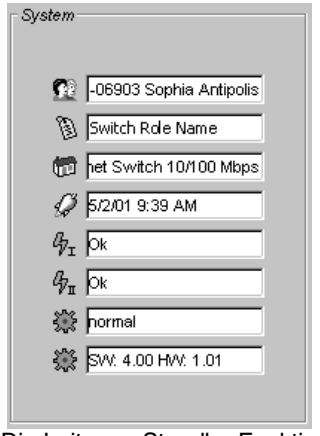
Aufzeichnung

Dieser Bereich der Startseite zeigt den Ereignisspeicher für den NxS. Da der Ereignisspeicher vom Webbrowser-Applet gewartet wird, steht er nur während der Laufzeit des Applets zur Verfügung.
Die folgenden Abbildung zeigt die Komponenten der Ereignisspeicher-Anzeige.



System

Dieser Bereich der Startseite zeigt den System-Ereignisspeicher des Agenten.
Die folgende Abbildung zeigt die Komponenten der Systemparameter-Anzeige.



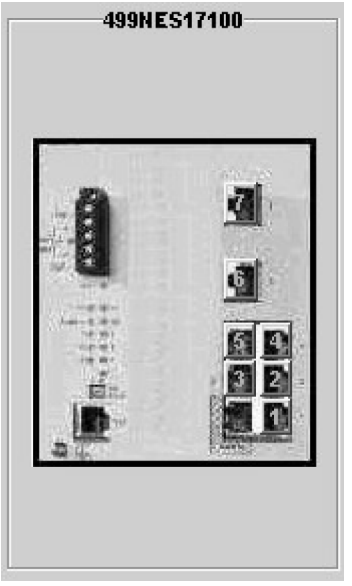
– Die Kontaktperson für diesen Switch
– Der Name dieses Switches
– Die Lage dieses Switches
– Datum und Zeit der Aktivierung des Switch
– Status von Spannungsversorgung 1
– Status von Spannungsversorgung 2
– Standby-/Redundanzfunktion des Switch
– Software- und Hardwareversion

Die Leitungs-Standby-Funktion zeigt den aktuellen Betriebszustand des NxS im Bezug auf die redundante Verbindung zwischen zwei Netzwerken (siehe *Redundante Kopplung von Netzwerksegmenten, S. 57*).

Normal	Normale Switch-Funktion
Standby inaktiv	Die Hauptleitung zwischen den beiden Netzwerken ist einwandfrei Der NxS ist passiv.
Standby inaktiv	Störung in der Hauptleitung zwischen den beiden Netzwerken. Der NxS hat die redundante Leitung aktiviert.
Nur NxS17100:	
Redundanz inaktiv	Der integrierte Redundanz-Manager ist aktiv
Redundanz inaktiv	Der integrierte Redundanz-Manager ist nicht aktiv

Ansicht des Switch

Dieser Bereich der Startseite zeigt eine Abbildung des Switch. Die genaue Beschreibung des Switch steht über der Abbildung.



Aktualisierung

Dieser Bereich wird angezeigt, wenn die Daten vom NxS im Browser automatisch aktualisiert werden. Durch Anklicken der Schaltfläche "reload Now!" werden diese Daten sofort aktualisiert. Standardmäßig werden die Daten alle 100 Sekunden aktualisiert.

Konfiguration

Der Konfigurationsbereich besteht aus zwei Registerkarten:

- Anschluss
- System

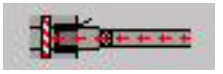
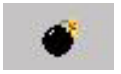
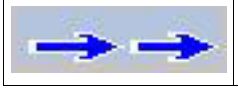
Anschluss

Die Registerkarte "Anschluss" bietet zwei Ansichten:

- Alle Anschlüsse zusammen und
- jeden Anschluss einzeln

Anschluss-registersymbole

Die folgenden Tabelle beschreibt die Bedeutung der Anschlussregistersymbole.

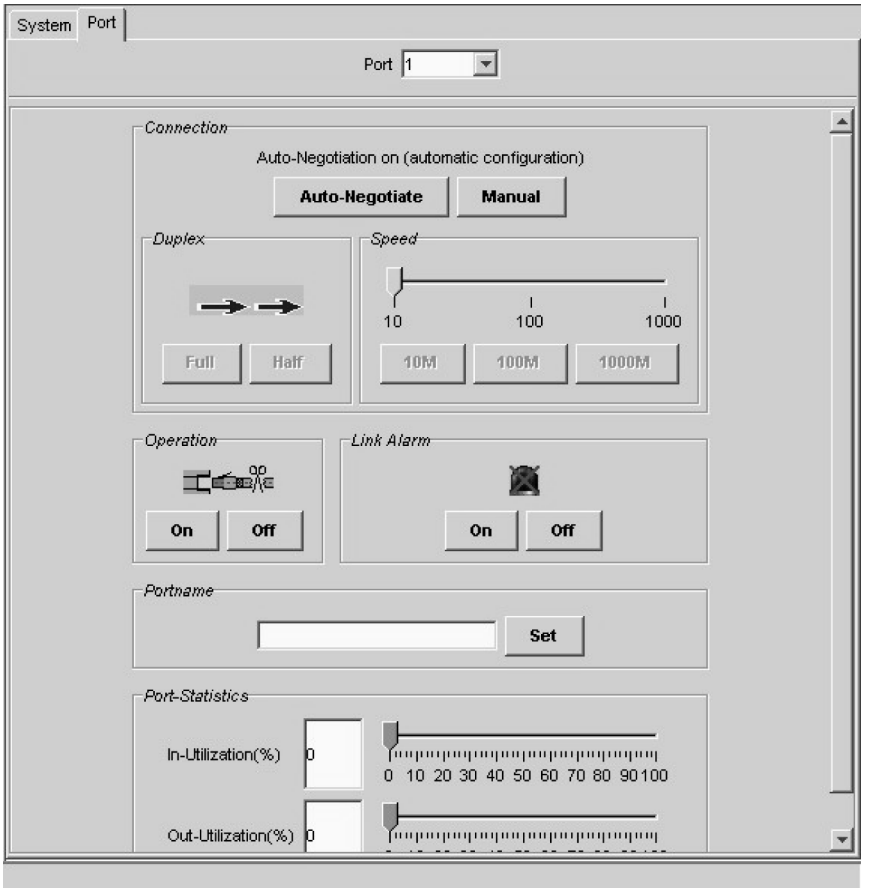
Symbol	Bedeutung
	Der Anschluss ist freigegeben und die Verbindung ist einwandfrei.
	Der Anschluss wird entweder vom Netzwerkmanagement oder von der Redundanzsteuerung gesperrt. Ein Anschluss kann nur vom Netzwerkmanagement und der Redundanzsteuerung freigegeben werden.
	Der Anschluss ist freigegeben und die Verbindung ist unterbrochen.
	Der NxS kann nicht erreicht werden. Möglicherweise wurde ein falsches Passwort eingegeben.
	Der von einem Verbindungsfehler ausgelöste Trap ist deaktiviert.
	Der von einem Verbindungsfehler ausgelöste Trap ist aktiviert.
	Anschluss arbeitet im Vollduplexmodus.
	Anschluss arbeitet im Halbduplexmodus.

Für die Ringredundanz sind an den Anschlüssen 6 und 7 die folgenden Einstellungen erforderlich (Siehe *Redundante Kopplung von Netzwerksegmenten, S. 57*):

- 100 Mbps
- Vollduplex
- Automatische Einstellung aus
- Betrieb ein.

Einzelanschluss-konfiguration

Die folgende Abbildung zeigt den Bildschirm für die Einzelanschlusskonfiguration.



Die Zeile **Name** die angibt, dass der Anschluss als Einzelanschluss beschrieben wird. Hier können Sie einen beliebigen Text eintragen, z.B. den Benutzernamen des angeschlossenen Geräts.

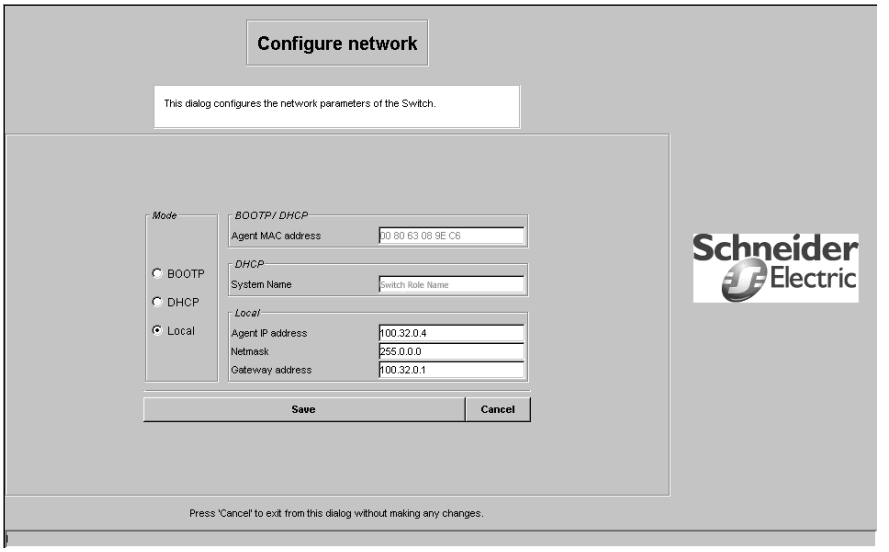
System-konfiguration

Das Dateikartensystem ermöglicht folgende Funktionen:

- das Netzwerk konfigurieren...
- die Systeminformationen ändern...
- die Konfiguration laden/speichern...
- die Anschlussspiegelung durchführen...
- die Software aktualisieren...
- Rücksetzung
- das Passwort ändern...

Netzwerk konfigurieren

Die folgende Abbildung zeigt die Seite "Netzwerk konfigurieren".



Erforderliche Schritte beim Konfigurieren des Netzwerks

Mit den folgenden Schritten weisen Sie auf der Seite "Netzwerk konfigurieren" Netzwerkparameter zu.

Schritt	Aktion
1	Geben Sie unter **Modus**ein, wie dem NxS seine IP-Parameter zugewiesen werden sollen • BOOTP (siehe *BOOTP (BOOTstrap-Protokoll), S. 28*) • DHCP (siehe *DHCP-Protokoll, S. 29*) • Lokal.
2	Geben Sie die Parameter entsprechend des rechts gewählten Modus ein.

Konfiguration laden/speichern

In diesem Fenster können Sie eine benutzerdefinierte Konfiguration speichern. Diese Konfiguration kann erneut geladen werden;

- entweder automatisch beim erneuten Laden oder
- nach dem erneuten Laden mit den Grundeinstellungen.

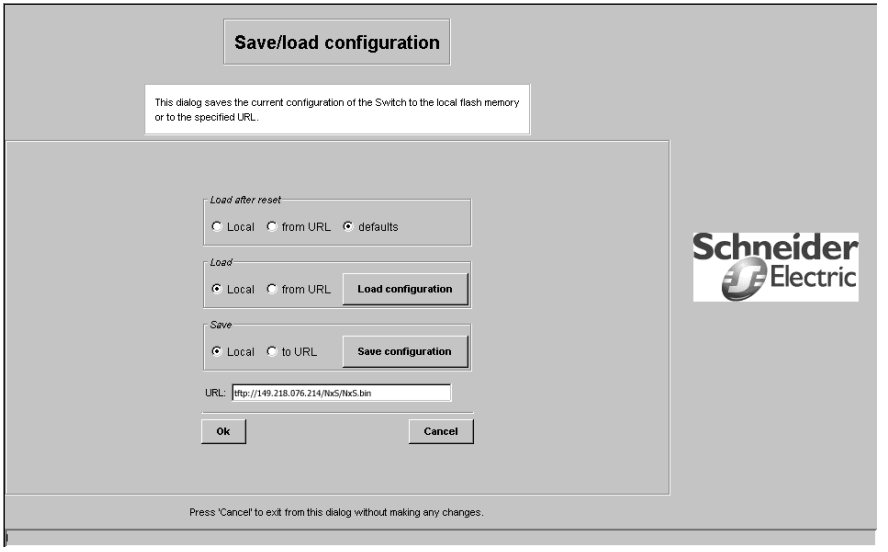
Die Konfiguration kann entweder gespeichert oder im Flash-Speicher bzw. in einem TFTP-Server abgelegt werden.

Der Pfad für die Speicherung der Konfigurationsdaten wird in der Zeile "URL" angezeigt.

Das TFTP-Protokoll kann keine neue Datei erstellen. Daher muss auf dem TFTP-Server eine leere Datei erstellt werden, bevor Sie die Daten unter der URL abspeichern.

Auf einem TFTP-Server speichern

Die folgende Abbildung zeigt den Bildschirm "Konfiguration sichern/laden".



Erforderliche Schritte beim Speichern auf einem TFTP-Server

Mit den folgenden Schritten speichern Sie auf einem TFTP-Server.

Schritt	Aktion
1	Öffnen sie eine neue Datei mit einem beliebigen Editor.
2	Speichern Sie die leere Datei unter dem jeweiligen Pfad des TFTP-Servers einschließlich Dateiname, z.B. **RAM0/Switch_Role_Name.prm**
3	Geben Sie auf der Zeile "URL" den Pfad des TFTP-Servers ein, z.B. **tftp://149.218.076.214/RAM0/Switch_Role_Name.prm**.

Zugriffs-sicherheit des TFTP-Servers

Die Konfigurationsdatei enthält alle Konfigurationsdaten einschließlich Passwort. Dies ist bei der Erteilung der Zugriffsrechte auf dem TFTP-Server zu beachten.

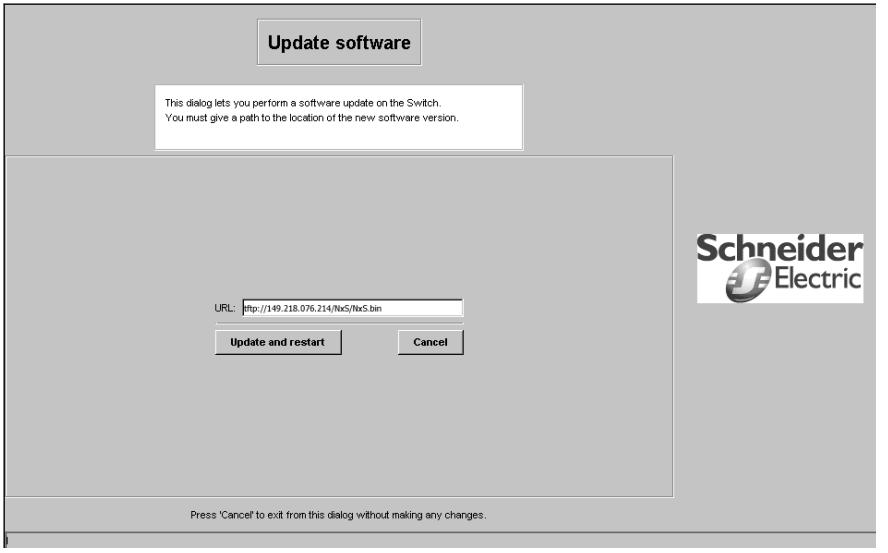
Anschluss-spiegelung

Daten, die über die beiden von Ihnen in diesem Menü gewählten Anschlüsse eingehen, werden an die übrigen Anschlüsse weitergeleitet.
Auf diese Weise können Sie von jedem Anschluss des NxS die Kommunikation zwischen zwei oder mehr Geräten verfolgen. Die Geräte können direkt oder indirekt über einen Hub mit diesen Anschlüssen verbunden werden.
Die Verwendung eines Analysators ist möglich, um Datenübertragungsblöcke einer bestimmten Kommunikationsbeziehung zu filtern und zu analysieren.

Hinweis: Nur mit NxS17100 verfügbar.

Software aktualisieren

Ehe Sie die Software aktualisieren können, müssen Sie den genauen Speicherort bzw. den Pfad der Aktualisierungsdatei kennen. Die folgende Abbildung zeigt den Bildschirm "Software aktualisieren".


Update software
This dialog lets you perform a software update on the Switch.
You must give a path to the location of the new software version.
URL:
http://149.218.076.214/NxS/NxS.bin
Update and restart
Cancel
Schneider Electric
Press 'Cancel' to exit from this dialog without making any changes.

Erforderliche Schritte bei der Aktualisierung der Software

Gehen Sie bei der Aktualisierung der Software wie im folgenden beschrieben vor.

Schritt	Aktion	Kommentar
1	Tragen Sie den korrekten Pfadnamen in das URL–Feld ein und klicken Sie auf **Aktualisieren**.	Beispiel für einen Pfadnamen: tftp://149.218.076.214/NxS/NxS.bin
2	Laden Sie die aktualisierten Seiten nach der Aktualisierung der Software erneut vom Switch.	Nach einem Neustart kann Ihr Browser die neue Version der webbasierten Schnittstelle laden. Um zu verhindern, dass eine alte Interface-Seite aus dem Cache verwendet wird, muss der Browser eventuell so eingestellt werden, dass er auf den Switch zugreift und die aktualisierte Seite lädt. Die meisten Browser verfügen über eine Funktionsleiste, ein Menü und Tastaturbefehle zum Aktualisieren oder Neuladen. (Beim Internet Explorer **F5**drücken.

Passwort ändern

Mit den folgenden Schritten können Sie das Passwort ändern.

Schritt	Aktion
1	Tragen Sie das neue Passwort in die Zeile **Neues Passwort** ein.
2	Tragen Sie das neue Passwort erneut in die Zeile **Bitte erneut eingeben** ein. Bitte denken Sie daran, dass bei Passwörtern die Groß- und Kleinschreibung zu beachten ist.

Verwaltungsinformationsbasis (MIB)

6

Auf einen Blick

Übersicht

Dieses Kapitel enthält Informationen über die Entwicklung, Struktur, Abkürzungen, Begriffe, Objektgruppen und Konfiguration von Eigenschaften der Verwaltungsinformationsbasis (MIB, Management Information Base).

Inhalt dieses Kapitels

Dieses Kapitel enthält die folgenden Themen:

Thema	Seite
Verwaltungsinformationsbasis (MIB)	80
MIB II	83
Private MIB	95

Verwaltungsinformationsbasis (MIB)

Übersicht

Die Entwicklungsgrundlage der Verwaltungsinformationsbasis (**M**anagement **I**nformation **B**ase, MIB) ist eine abstrakte Baumstruktur.
Die Verzweigungspunkte sind die **Objektklassen**. Die "Blätter" der MIB werden als **generische Objektklassen** bezeichnet. Wenn eine eindeutige Identifizierung notwendig ist, werden die generischen Objektklassen **instanziert**, d. h., die abstrakte Struktur wird real abgebildet, indem die Portadresse oder die Zieladresse angegeben wird.
Diesen Instanzen werden Werte (Ganzzahlen, Zeittakte, Zähler oder Bytefolgen) zugewiesen, die gelesen und in manchen Fällen geändert werden können. Durch die **Objektbeschreibung** oder **Objekt-ID** (OID) wird die Objektklasse identifiziert. Der Nebenbezeichner (Subidentifier, SID) wird für die Instanzierung verwendet.

Beispiel:
Die generische Objektklasse
`saPSState (OID = 1.3.6.1.4.1.3833.1.1.14.1.2.1.3)`

ist die Beschreibung der abstrakten Information "Stromversorgungsstatus". Es ist jedoch nicht möglich, hieraus eine Information abzuleiten, da das System nicht weiß, welche Stromversorgung gemeint ist.
Durch Angabe des Nebenbezeichners (2) wird diese abstrakte Information real abgebildet (instanziert), was bedeutet, dass sich die Information auf die Stromversorgung 2 bezieht. Dieser Instanz wird ein Wert zugewiesen, der dann gelesen werden kann. Beispielsweise gibt Instanz "get 1.3.6.1.4.1.3833.1.1.14.1.2.1.3" die Antwort "1" zurück, was bedeutet, dass die Stromversorgung in Ordnung ist.

MIB-Abkürzungen

In der folgenden Tabelle werden die Abkürzungen definiert, die in der MIB verwendet werden.

Abkürzung	Bedeutung
Comm	Gruppenzugriffsberechtigungen
con	Konfiguration
Descr	Beschreibung
Fan	Fan
ID	Bezeichner
Lwr	Unterer (z.B. Schwellenwert)
PS	Stromversorgung
Pwr	Versorgungsspannung
sys	System
UI	Benutzerschnittstelle
Upr	Oberer (z.B. Schwellenwert)
ven	Hersteller (Schneider Automation)

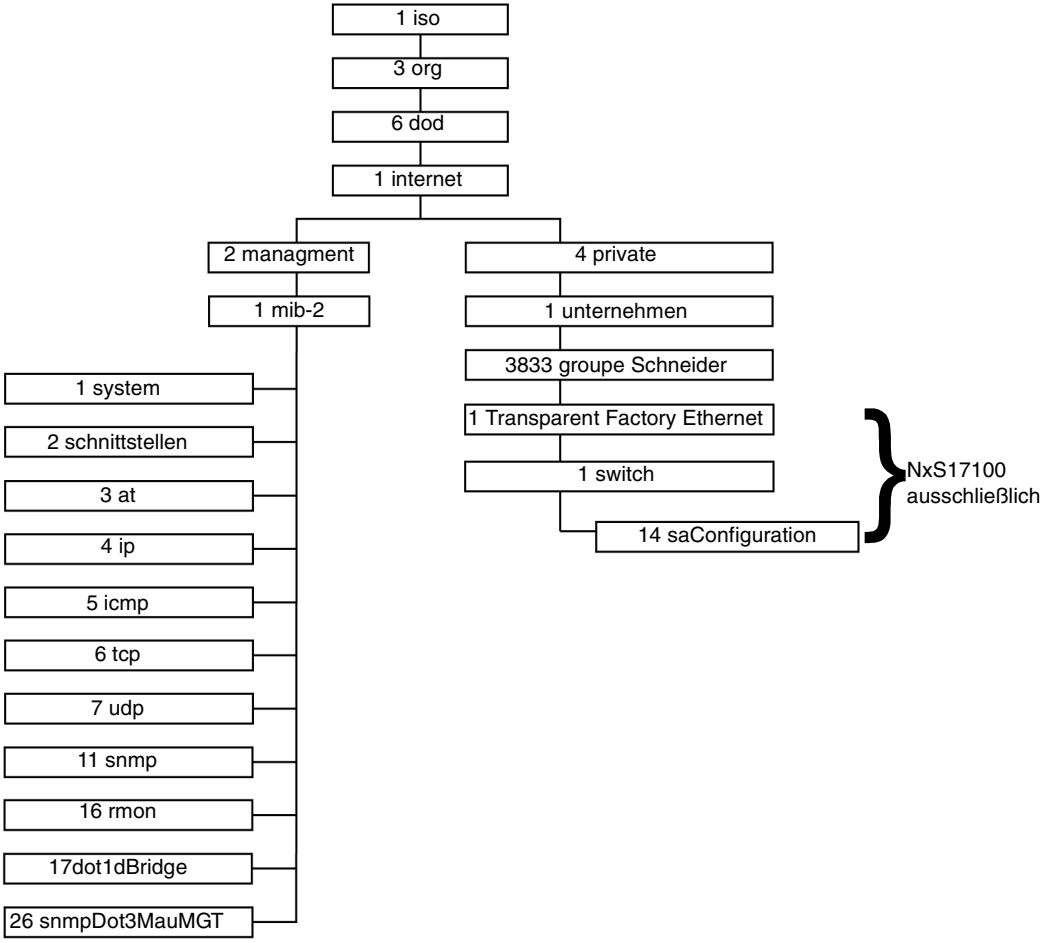
Syntax-definitionen

In der folgenden Tabelle werden die Syntaxbegriffe definiert, die in der MIB verwendet werden.

Begriff	Definition
Integer	Eine Ganzzahl im Bereich von 0 - 2^{32}
IP address	IP-Adresse: xxx.xxx.xxx.xxx (xxx = Ganzzahl im Bereich von 0 - 255)
MAC address	MAC-Adresse: 12-stellige Hexadezimalzahl gemäß ISO/IEC 8802-3
Object Identifier	Objekt-ID: x.x.x.x ... (z. B. 1.3.6.1.1.4.1.3833 ...)
Octet String	ASCII-Zeichenkette
PSID	Stromversorgungsbezeichner (Stromversorgungsnummer)
TimeTicks	Stoppuhr Abgelaufene Zeit (in Sekunden) = numerischer Wert / 100 Numerischer Wert = Ganzzahl im Bereich von 0 - 2^{32}
Timeout	Zeitwert in Hundertstelsekunden Zeitwert = Ganzzahl im Bereich von 0 - 2^{32}
Typefield	4-stellige Hexadezimalzahl gemäß ISO/IEC 8802-3
Counter	Ganzzahl (0 - 2^{32}), deren Wert um 1 heraufgesetzt wird, wenn bestimmte Ereignisse auftreten.

MIB-Baumstruktur

Im folgenden Ablaufdiagramm wird die Baumstruktur der Switch-MIB dargestellt.



Hinweis: Nicht alle Geräte unterstützen alle Objektklassen. Der Wert "nicht unterstützt" (not supported) wird zurückgegeben, wenn eine nicht unterstützte Objektklasse angefordert wird. Ein Versuch, eine nicht unterstützte Objektklasse zu ändern, resultiert in der Meldung "badValue" (ungültiger Wert).

MIB II

Systemgruppe (1.3.6.1.2.1.1)

Die Systemgruppe ist eine Gruppe, die für alle Systeme erforderlich ist. Sie enthält systembezogene Objekte. Wenn ein Agent keinen Wert für eine Variable hat, enthält die zurückgegebene Anwort eine Zeichenkette mit der Länge 0.

```
(1) system
    |-- (1) sysDescr
    |-- (2) sysObjectID
    |-- (3) sysUpTime
    |-- (4) sysContact
    |-- (5) sysName
    |-- (6) sysLocation
    |-- (7) sysServices
```

Systemgruppen-objekte In der folgenden Abbildung werden die Objekte der Systemgruppe beschrieben.

Objekt	OID	Syntax	Zugriff	Beschreibung
sysDescr	1.3.6.1.2 .1.1.1.0	ASCII-Zeichenkette (Größe: 0-255)	Lesen	Eine verbale Beschreibung des Eintrags. Dieser Wert sollte den vollständigen Namen und die Versionsnummer des Typs der Systemhardware, der Software des Betriebssystems und der Netzwerksoftware enthalten. Die Beschreibung darf nur aus druckbaren ASCII-Zeichen bestehen.
sysObjectID	1.3.6.1.2 .1.1.2.0	Objektbezeichner	Lesen	Die Berechtigungsidentifizierung des Herstellers des Netzverwaltungssystems, das in dieses Gerät integriert ist. Der Wert wird in den SMI-Unternehmenszweig (1.3.6.1.4.1) eingetragen und beschreibt, welcher Gerätetyp verwaltet wird. Zum Beispiel: Wenn der Hersteller "Schneider Electric" dem Zweig 1.3.6.1.4.1.3833 zugewiesen ist, kann er seinem Switch den Bezeichner 1.3.6.1.4.1.3833.1.1 zuweisen.
sysUpTime	1.3.6.1.2 .1.1.3.0	Zeittakte	Lesen	Die Zeit in 1/100 Sekunden seit der letzten Rücksetzung der Netzverwaltungseinheit.
sysContact	1.3.6.1.2 .1.1.4.0	ASCII-Zeichenkette (Größe: 0-255)	Lesen und Schreiben	Die Klartextidentifizierung der Kontaktperson für den betreffenden verwalteten Teilnehmer mit Informationen, wie diese Person zu kontaktieren ist.
sysName	1.3.6.1.2 .1.1.5.0	ASCII-Zeichenkette (Größe: 0-255)	Lesen und Schreiben	Ein Name für diesen Teilnehmer, um ihn für die Verwaltung zu identifizieren. Gemäß Programmkonvention ist dies der voll qualifizierte Name in der Domäne.
sysLocation	1.3.6.1.2 .1.1.6.0	ASCII-Zeichenkette (Größe: 0-255)	Lesen und Schreiben	Der physische Ort des betreffenden Teilnehmers (z.B. "Treppe, dritter Stock")
sysServices	1.3.6.1.2 .1.1.7.0	Ganzzahl (0 - 127)	Lesen	Dieser Wert zeigt die vom Teilnehmer angebotenen Dienste an. Es handelt sich um einen Integralwert, der durch die Summenbildung von $2^{(Schicht - 1)}$ für jede der ISO-Schichten, für die vom Teilnehmer Dienste bereitstellt werden, berechnet wird. Zum Beispiel: Ein Teilnehmer stellt Routing-Funktionen (OSI-Schicht 3) bereit: sysServices = $2^{(3-1)} = 4$ Ein Teilnehmer ist ein Host und stellt Anwendungs- und Netzdienste (OSI-Schichten 4 und 7) bereit: sysServices = $2^{(4-1)} + 2^{(7-1)} = 72$

Schnittstellengruppe (1.3.6.1.2.1.2)

Die Schnittstellengruppe enthält Informationen über die Geräteschnittstellen.

```
(2) interfaces
    |-- (1) ifNumber
    |-- (2) ifTable
        |-- (1) ifEntry
            |-- (1) ifIndex
            |-- (2) ifDescr
            |-- (3) ifType
            |-- (4) ifMtu
            |-- (5) ifSpeed
            |-- (6) ifPhysAddress
            |-- (7) ifAdminStatus
            |-- (8) ifOperStatus
            |-- (9) ifLastChange
            |-- (10) ifInOctets
            |-- (11) ifInUcastPkts
            |-- (12) ifInNUcastPkts
            |-- (13) ifInDiscards
            |-- (14) ifInErrors
            |-- (15) ifInUnknownProtos
            |-- (16) ifOutOctets
            |-- (17) ifOutUcastPkts
            |-- (18) ifOutNUcastPkts
            |-- (19) ifOutDiscards
            |-- (20) ifOutErrors
            |-- (21) ifOutQLen
            |-- (22) ifSpecific
```

Adressumsetzungsgruppe (1.3.6.1.2.1.3)

Die Adressumsetzungsgruppe wird für alle Systeme benötigt. Sie enthält Informationen über die Zuweisung von Adressen.

```
(3) at
    |-- (1) atTable
        |-- (1) atEntry
            |-- (1) atIfIndex
            |-- (2) atPhysAddress
            |-- (3) atNetAddress
```

IP-Gruppe (1.3.6.1.2.1.4)

Die IP-Gruppe (Internet Protocol Group, Internetprotokollgruppe) wird für alle Systeme benötigt. Sie enthält Informationen, die sich auf die IP-Vermittlung auswirken.

```
(4) ip
    |-- (1) ipForwarding
    |-- (2) ipDefaultTTL
    |-- (3) ipInReceives
    |-- (4) ipInHdrErrors
    |-- (5) ipInAddrErrors
    |-- (6) ipForwDatagrams
    |-- (7) ipInUnknownProtos
    |-- (8) ipInDiscards
    |-- (9) ipInDelivers
    |-- (10) ipOutRequests
    |-- (11) ipOutDiscards
    |-- (12) ipOutNoRoutes
    |-- (13) ipReasmTimeout
    |-- (14) ipReasmReqds
    |-- (15) ipReasmOKs
    |-- (16) ipReasmFails
    |-- (17) ipFragOKs
    |-- (18) ipFragFails
    |-- (19) ipFragCreates
    |-- (20) ipAddrTable
    |   |-- (1) ipAddrEntry
            |-- (1) ipAdEntAddr
            |-- (2) ipAdEntIfIndex
            |-- (3) ipAdEntNetMask
            |-- (4) ipAdEntBcastAddr
            |-- (5) ipAdEntReasmMaxSize
    |-- (21) ipRouteTable
    |   |-- (1) ipRouteEntry
            |-- (1) ipRouteDest
            |-- (2) ipRouteIfIndex
            |-- (3) ipRouteMetric1
            |-- (4) ipRouteMetric2
            |-- (5) ipRouteMetric3
            |-- (6) ipRouteMetric4
            |-- (7) ipRouteNextHop
            |-- (8) ipRouteType
            |-- (9) ipRouteProto
            |-- (10) ipRouteAge
            |-- (11) ipRouteMask
            |-- (12) ipRouteMetric5
```

```
            |-- (13) ipRouteInfo
    |-- (22) ipNetToMediaTable
    |   |-- (1) ipNetToMediaEntry
    |       |-- (1) ipNetToMediaIfIndex
    |       |-- (2) ipNetToMediaPhysAddress
    |       |-- (3) ipNetToMediaNetAddress
    |       |-- (4) ipNetToMediaType
    |-- (23) ipRoutingDiscards
```

ICMP-Gruppe (1.3.6.1.2.1.5)

Die ICMP-Gruppe (Internet Control Message Protocol Group, Internetsteuerungsprotokoll-Gruppe) ist für alle Systeme obligatorisch. Sie enthält alle Informationen zur Fehlerbehandlung und Steuerung für den Datenaustausch im Internet.

```
(5) icmp
    |-- (1) icmpInMsgs
    |-- (2) icmpInMsgs
    |-- (3) icmpInDestUnreachs
    |-- (4) icmpInTimeExcds
    |-- (5) icmpInParmProbs
    |-- (6) icmpInSrcQuenchs
    |-- (7) icmpInRedirects
    |-- (8) icmpInEchos
    |-- (9) icmpInEchoReps
    |-- (10) icmpInTimestamps
    |-- (11) icmpInTimestampReps
    |-- (12) icmpInAddrMasks
    |-- (13) icmpInAddrMaskReps
    |-- (14) icmpOutMsgs
    |-- (15) icmpOutErrors
    |-- (16) icmpOutDestUnreachs
    |-- (17) icmpOutTimeExcds
    |-- (18) icmpOutParmProbs
    |-- (19) icmpOutSrcQuenchs
    |-- (20) icmpOutRedirects
    |-- (21) icmpOutEchos
    |-- (22) icmpOutEchoReps
    |-- (23) icmpOutTimestamps
    |-- (24) icmpOutTimestampReps
    |-- (25) icmpOutAddrMasks
    |-- (26) icmpOutAddrMaskReps
```

TCP-Gruppe (1.3.6.1.2.1.6)

Die TCP-Gruppe (Transfer Control Protocol Group, Transfersteuerungsprotokoll-Gruppe) ist für alle Systeme erforderlich, bei denen TCP implementiert ist. Spezielle Objekte zur Beschreibung von Informationen zu einer bestimmten TCP-Verbindung existieren nur solange, wie die Verbindung vorhanden ist.

```
(6) tcp
    |-- (1) tcpRtoAlgorithm
    |-- (2) tcpRtoMin
    |-- (3) tcpRtoMax
    |-- (4) tcpMaxConn
    |-- (5) tcpActiveOpens
    |-- (6) tcpPassiveOpens
    |-- (7) tcpAttemptFails
    |-- (8) tcpEstabResets
    |-- (9) tcpCurrEstab
    |-- (10) tcpInSegs
    |-- (11) tcpOutSegs
    |-- (12) tcpRetransSegs
    |-- (13) tcpConnTable
    |    |-- (1) tcpConnEntry
    |        |-- (1) tcpConnState
    |        |-- (2) tcpConnLocalAddress
    |        |-- (3) tcpConnLocalPort
    |        |-- (4) tcpConnRemAddress
    |        |-- (5) tcpConnRemPort
    |-- (14) tcpInErrs
    |-- (15) tcpOutRsts
```

UDP-Gruppe (1.3.6.1.2.1.7)

Die UDP-Gruppe (User Datagram Protocol Group, Benutzerdatagrammprotokoll-Gruppe) ist für alle Systeme erforderlich, bei denen UDP implementiert ist.

```
(7) udp
    |-- (1) udpInDatagrams
    |-- (2) udpNoPorts
    |-- (3) udpInErrors
    |-- (4) udpOutDatagrams
    |-- (5) udpTable
    |    |-- (1) udpEntry
    |        |-- (1) udpLocalAddress
    |        |-- (2) udpLocalPort
```

SNMP-Gruppe (1.3.6.1.2.1.11)

Die SNMP-Gruppe (Simple Network Management Protocol Group, Einfaches-Netzverwaltungsprotokoll-Gruppe) ist für alle Systeme erforderlich. In SNMP-Installationen, die optimiert worden sind, um entweder einen Agenten oder eine Verwaltungsstation zu unterstützen, enthalten einige der aufgelisteten Objekte den Wert "0".

```
(11) snmp
     |-- (1) snmpInPkts
     |-- (2) snmpOutPkts
     |-- (3) snmpInBadVersions
     |-- (4) snmpInBadCommunityNames
     |-- (5) snmpInBadCommunityUses
     |-- (6) snmpInASNParseErrs
     |-- (7) not used
     |-- (8) snmpInTooBigs
     |-- (9) snmpInNoSuchNames
     |-- (10) snmpInBadValues
     |-- (11) snmpInReadOnlys
     |-- (12) snmpInGenErrs
     |-- (13) snmpInTotalReqVars
     |-- (14) snmpInTotalSetVars
     |-- (15) snmpInGetRequests
     |-- (16) snmpInGetNexts
     |-- (17) snmpInSetRequests
     |-- (18) snmpInGetResponses
     |-- (19) snmpInTraps
     |-- (20) snmpOutTooBigs
     |-- (21) snmpOutNoSuchNames
     |-- (22) snmpOutBadValues
     |-- (23) not used
     |-- (24) snmpOutGenErrs
     |-- (25) snmpOutGetRequests
     |-- (26) snmpOutGetNexts
     |-- (27) snmpOutSetRequests
     |-- (28) snmpOutGetResponses
     |-- (29) snmpOutTraps
     |-- (30) snmpEnableAuthenTraps
```

RMON-Gruppe (1.3.6.1.2.1.16)

Dieser Teil der MIB sorgt für einen kontinuierlichen Fluss der aktuellen und historischen Netzkomponentendaten zur Netzwerkverwaltung. Durch die Konfiguration von Alarmen und Ereignissen wird die Bewertung der Netzkomponentenzähler gesteuert. Die Agenten informieren die Verwaltungsstation je nach Konfiguration durch Traps über das Bewertungsergebnis.

```
(16) rmon
    |--(1) statistics
        |--(1) etherStatsTable
            |--(1) etherStatsEntry
                |--(1) etherStatsIndex
                |--(2) etherStatsDataSource
                |--(3) etherStatsDropEvents
                |--(4) etherStatsOctets
                |--(5) etherStatsPkts
                |--(6) etherStatsBroadcastPkts
                |--(7) etherStatsMulticastPkts
                |--(8) etherStatsCRCAlignErrors
                |--(9) etherStatsUndersizePkts
                |--(10) etherStatsOversizePkts
                |--(11) etherStatsFragments
                |--(12) etherStatsJabbers
                |--(13) etherStatsCollisions
                |--(14) etherStatsPkts64Octets
                |--(15) etherStatsPkts65to127Octets
                |--(16) etherStatsPkts128to255Octets
                |--(17) etherStatsPkts256to511Octets
                |--(18) etherStatsPkts512to1023Octets
                |--(19) etherStatsPkts1024to1518Octets
                |--(20) etherStatsOwner
                |--(21) etherStatsStatus
    |--(2) history
        |--(1) historyControlTable
            |--(1) historyControlEntry
                |--(1) historyControlIndex
                |--(2) historyControlDataSource
                |--(3) historyControlBucketsRequested
                |--(4) historyControlBucketsGranted
                |--(5) historyControlInterval
                |--(6) historyControlOwner
                |--(7) historyControlStatus
        |--(2) etherHistoryTable
            |--(1) etherHistoryEntry
                |--(1) etherHistoryIndex
                |--(2) etherHistorySampleIndex
```

```
                |--(3) etherHistoryIntervalStart
                |--(4) etherHistoryDropEvents
                |--(5) etherHistoryOctets
                |--(6) etherHistoryPkts
                |--(7) etherHistoryBroadcastPkts
                |--(8) etherHistoryMulticastPkts
                |--(9) etherHistoryCRCAlignErrors
                |--(10) etherHistoryUndersizePkts
                |--(11) etherHistoryOversizePkts
                |--(12) etherHistoryFragments
                |--(13) etherHistoryJabbers
                |--(14) etherHistoryCollisions
                |--(15) etherHistoryUtilization
    |--(3) alarm
        |--(1) alarmTable
            |--(1) alarmEntry
                |--(1) alarmIndex
                |--(2) alarmInterval
                |--(3) alarmVariable
                |--(4) alarmSampleType
                |--(5) alarmValue
                |--(6) alarmStartupAlarm
                |--(7) alarmRisingThreshold
                |--(8) alarmFallingThreshold
                |--(9) alarmRisingEventIndex
                |--(10) alarmFallingEventIndex
                |--(11) alarmOwner
                |--(12) alarmStatus
    |--(9) event
        |--(1) eventTable
            |--(1) eventEntry
                |--(1) eventIndex
                |--(2) eventDescription
                |--(3) eventType
                |--(4) eventCommunity
                |--(5) eventLastTimeSent
                |--(6) eventOwner
                |--(7) eventStatus
        |--(2) logTable
            |--(1) logEntry(1)
                |--(1) logEventIndex
                |--(2) logIndex
                |--(3) logTime
                |--(4) logDescription
```

dot1dBridge (1.3.6.1.2.1.17)

Dieser Teil der MIB enthält Bridge-spezifische Objekte.

```
(17) dot1dBridge
    |--(1) dot1dBase
        |--(1) dot1dBaseBridgeAddress
        |--(2) dot1dBaseNumPorts
        |--(3) dot1dBaseType
        |--(4) dot1dBasePortTable
            |--(1) dot1dBasePortEntry
                |--(1) dot1dBasePort
                |--(2) dot1dBasePortIfIndex
                |--(3) dot1dBasePortCircuit
                |--(4) dot1dBasePortDelayExceededDiscards
                |--(5) dot1dBasePortMtuExceededDiscards
    |--(2) dot1dStp
    |--(3) dot1dSr
    |--(4) dot1dTp
        |--(1) dot1dTpLearnedEntryDiscards
        |--(2) dot1dTpAgingTime
        |--(3) dot1dTpFdbTable
            |--(1) dot1dTpFdbEntry
                |--(1) dot1dTpFdbAddress
                |--(2) dot1dTpFdbPort
                |--(3) dot1dTpFdbStatus
        |--(4) dot1dTpPortTable
            |--(1) dot1dTpPortEntry
                |--(1) dot1dTpPort
                |--(2) dot1dTpPortMaxInfo
                |--(3) dot1dTpPortInFrames
                |--(4) dot1dTpPortOutFrames
                |--(5) dot1dTpPortInDiscards
    |--(5) dot1dStatic
        |--(1) dot1dStaticTable
            |--(1) dot1dStaticEntry
                |--(1) dot1dStaticAddress
                |--(2) dot1dStaticReceivePort
                |--(3) dot1dStaticAllowedToGoTo
                |--(4)  dot1dStaticStatus
    |--(6) pBridgeMIB
        |--(1) pBridgeMIBObjects
            |--(1) dot1dExtBase
                |--(1) dot1dDeviceCapabilities
                |--(2) dot1dTrafficClassesEnabled
                |--(3) dot1dGmrpStatus
                |--(4) dot1dPortCapabilitiesTable
```

```
                        |--(1) dot1dPortCapabilitiesEntry
                            |--(1) dot1dPortCapabilities
                |--(3) dot1dGarp
                    |--(1) dot1dPortGarpTable
                        |--(1) dot1dPortGarpEntry
                            |--(1) dot1dPortGarpJoinTime
                            |--(2) dot1dPortGarpLeaveTime
                            |--(3) dot1dPortGarpLeaveAllTime
                |--(4) dot1dGmrp
                    |--(1) dot1dPortGmrpTable
                        |--(1) dot1dPortGmrpEntry
                            |--(1) dot1dPortGmrpStatus
                          |--(2) dot1dPortGmrpFailedRegistrations
                            |--(3) dot1dPortGmrpLastPduOrigin
    |--(7) qBridgeMIB
        |--(1) qBridgeMIBObjects
            |--(2) dot1qTp
                |--(3) dot1qTpGroupTable
                    |--(1) dot1qTpGroupEntry
                        |--(1) dot1qTpGroupAddress
                        |--(2) dot1qTpGroupEgressPorts
                        |--(3) dot1qTpGroupLearnt
                |--(4) dot1qForwardAllTable
                    |--(1) dot1qForwardAllEntry
                        |--(1) dot1qForwardAllPorts
                        |--(2) dot1qForwardAllStaticPorts
                        |--(3) dot1qForwardAllForbiddenPorts
                |--(5) dot1qForwardUnregisteredTable
                    |--(1) dot1qForwardUnregisteredEntry
                        |--(1) dot1qForwardUnregisteredPorts
                    |--(2)dot1qForwardUnregisteredStaticPorts
                        |--(3)
dot1qForwardUnregisteredForbiddenPorts
```

MAU-Verwaltungs-gruppe (1.3.6.1.2.1.26)

Die MAU-Verwaltungsgruppe dient zum Festlegen der Parameter für die automatische Einstellung.

```
(26) snmpDot3MauMgt
    |-- (2) dot3IfMauBasicGroup
    |   |-- (1) ifMauTable
    |       |-- (1) ifMauEntry
    |           |-- (1) ifMauIfIndex
    |           |-- (2) ifMauIndex
    |           |-- (3) ifMauType
    |           |-- (4) ifMauStatus
    |           |-- (5) ifMauMediaAvailable
    |           |-- (6) ifMauMediaAvailableStateExits
    |           |-- (7) ifMauJabberState
    |           |-- (8) ifMauJabberingStateEnters
    |           |-- (9) ifMauFalseCarriers
    |           |-- (10)ifMauTypeList
    |           |-- (11)ifMauDefaultType
    |           |-- (12)ifMauAutoNegSupported
    |-- (5) dot3IfMauAutoNegGroup
    |   |-- (1) ifMauAutoNegTable
    |       |-- (1) ifMauAutoNegEntry
    |           |-- (1) ifMauAutoNegAdminStatus
    |           |-- (2) ifMauAutoNegRemoteSignaling
    |           |-- (4) ifMauAutoNegConfig
    |           |-- (5) ifMauAutoNegCapability
    |           |-- (6) ifMauAutoNegCapAdvertised
    |           |-- (7) ifMauAutoNegCapReceived
    |           |-- (8) ifMauAutoNegRestart
```

Private MIB

Übersicht

Die private MIB ist zum Konfigurieren der gerätespezifischen Eigenschaften des NxS vorgesehen. Die folgenden Gruppen werden im NxS anhand der saConfiguration (OID = 1.3.6.1.4.1.3833.1.1.14) der privaten MIB implementiert.

- saChassis (OID = 1.3.6.1.4.1.3833.1.1.14.1)
- saAgent (OID = 1.3.6.1.4.1.3833.1.1.14.2)
- userGroup (OID = 1.3.6.1.4.1.3833.1.1.14.3

Gerätegruppe

Die Gerätegruppe enthält Informationen über den Status der NxS-Hardware.

```
(14) saConfiguration
    |-- (1) saChassis
    |   |-- (1) saSystemTable
    |       |-- (1) saSysProduct
    |       |-- (2) saSysVersion
    |       |-- (3) saSysGroupCapacity
    |       |-- (4) saSysGroupMap
    |       |-- (5) saSysMaxPowerSupply
    |       |-- (6) saSysMaxFan
    |       |-- (7) saSysGroupModuleCapacity
    |       |-- (8) saSysModulePortCapacity
            |-- (9) saSysGroupTable
            |-- (11) saInterfaceTable
                |-- (1) saIfEntry
                    |-- (1) saIfaceGroupID
                    |-- (2) saIfaceID
                    |-- (3) saIfaceStpEnable
                    |-- (4) saIfaceLinkType
                    |-- (5) saIfaceAction
                    |-- (6) saIfaceNextHopMacAddress
                    |-- (7) saIfaceFlowControl
                    |-- (8) saIfacePriorityThreshold
                    |-- (9) saIfaceName
                    |-- (10) saIfaceTrunkID
            |-- (20) saSysChassisName
            |-- (21) saSysStpEnable
            |-- (22) saSysFlowControl
            |-- (23) saSysBOOTPEnable
            |-- (24) saSysDHCPEnable
            |-- (25) saSysTelnetEnable
            |-- (26) saSysHTTPEnable
    |   |-- (2) saPSTable
    |       |-- (1) saPSEntry
```

```
|           |-- (1) saPSSysID
|           |-- (2) saPSID
|           |-- (3) saPSState
|       |-- (5) saCurrentAddressTable
|           |-- (1) saCurrentAddressEntry
|               |-- (1) saCurrentAddress
|               |-- (2) saCurrentAddressReceivePort
|               |-- (3) saCurrentAddressStaticEgressPorts
|               |-- (4) saCurrentAddressEgressPorts
|               |-- (5) saCurrentAddressStatus
|   |-- (10) saNxSext
|       |-- (1) saNxSOperMode
|       |-- (2) saNxSConfigError
|       |-- (3) saNxSSigRelayState
|       |-- (4) saSigLinkTable
|           |-- (1) saSigLinkEntry
|               |-- (1) saSigLinkID
|               |-- (2) saSigLinkAlarm
|           |-- (5) saSigTrapReason
|           |-- (6) saSigReasonIndex
|           |-- (7) saNxSTopologyGroup
|               |-- (1) saNxSPartnerIpAddress
|               |-- (2) saNxSTopologyTable
|                   |-- (1) saNxSTopologyEntry
|                       |-- (1) saNxSTopologyLinkID
|                       |-- (2) saNxSTopologyIpAddress
|           |-- (8) saNxSConnectionMirroringGroup
|               |-- (1) saNxSConnectionMirroringStatus
|               |-- (2) saNxSConnectionMirroringPortOne
|               |-- (3) saNxSConnectionMirroringPortTwo
```

Verwaltungs-gruppe

Die Verwaltungsgruppe enthält Parameter zum Konfigurieren des Verwaltungsagenten.

```
(14)saConfiguration
    |-- (2) saAgent
    |   |-- (1) saAction
    |   |-- (2) saActionResult
    |   |-- (3) saNetwork
    |       |-- (1) saNetLocalIPAddr
    |       |-- (2) saNetLocalPhysAddr
    |       |-- (3) saNetGatewayIPAddr
    |       |-- (4) saNetMask
            |-- (7) saNetAction
    |   |-- (4) saFSTable
    |       |-- (1) saFSUpdFileName
    |       |-- (2) saFSConfFileName
    |       |-- (3) saFSLogFileName
    |       |-- (4) saFSUserName
    |       |-- (5) saFSTPPassword
    |       |-- (6) saFSAction
    |       |-- (8) saFSActionResult
            |-- (9) saFSBootConfiguration
            |-- (10) saFSRunningConfiguration
    |   |-- (7) saAuthGroup
    |       |-- (1) saAuthHostTableEntriesMax
    |       |-- (2) saAuthCommTableEntriesMax
    |       |-- (3) saAuthCommTable
    |           |-- (1) saAuthCommEntry
    |               |-- (1) saAuthCommIndex
    |               |-- (2) saAuthCommName
    |               |-- (3) saAuthCommPerm
    |               |-- (4) saAuthCommState
    |       |-- (4) saAuthHostTable
    |           |-- (1) saAuthHostEntry
    |               |-- (1) saAuthHostIndex
    |               |-- (2) saAuthHostName
    |               |-- (3) saAuthHostCommIndex
    |               |-- (4) saAuthHostIpAddress
    |               |-- (5) saAuthHostIpMask
    |               |-- (6) saAuthHostState
    |   |-- (8) saTrapGroup
    |       |-- (1) saTrapCommTableEntriesMax
    |       |-- (2) saTrapDestTableEntriesMax
    |       |-- (3) saTrapCommTable
    |           |-- (1) saTrapCommEntry
```

```
|                |-- (1) saTrapCommIndex
|                |-- (2) saTrapCommCommIndex
|                |-- (3) saTrapCommColdStart
|                |-- (4) saTrapCommLinkDown
|                |-- (5) saTrapCommLinkUp
|                |-- (6) saTrapCommAuthentication
|                |-- (7) saTrapCommBridge
|                |-- (8) saTrapCommRMON
|                |-- (9) saTrapCommUsergroup
|                |-- (10)saTrapCommDualHoming
|                |-- (11)saTrapCommChassis
|                |-- (12)saTrapCommState
|        |-- (4) saTrapDestTable
|            |-- (1) saTrapDestEntry
|                |-- (1) saTrapDestIndex
|                |-- (2) saTrapDestName
|                |-- (3) saTrapDestCommIndex
|                |-- (4) saTrapDestIpAddress
|                |-- (5) saTrapDestIpMask
|                |-- (6) saTrapDestState
|    |-- (9) saLastAccessGroup
|        |-- (1) saLastIpAddr
|        |-- (2) saLastPort
|        |-- (3) saLastCommunity
```

Benutzer-gruppen-Gruppe

Die Benutzergruppen-Gruppe enthält Parameter zum Konfigurieren der Benutzergruppenfunktionen.

```
(14) saConfiguration
    |-- (3) userGroup
        |-- (4) portSecurityTable
            |-- (1) portSecurityEntry
                |-- (1) portSecSlotID
                |-- (2) portSecPortID
                |-- (3) portSecPermission
                |-- (4) portSecAllowedUserID
                |-- (5) portSecAllowedGroupIDs
                |-- (6) portSecConnectedUserID
                |-- (7) portSecAction
```

Benutzerschnittstelle

7

Auf einen Blick

Übersicht

Die Benutzerschnittstelle ermöglicht Benutzern das Auswählen von bestimmten Funktionen des Verwaltungsagenten über Menüelemente.
Die folgenden Menüelemente können gewählt werden:

- Systemparameter
- Switchsicherheit
- Portkonfiguration
- Konfiguration
- Aktualisierung
- Ping
- Passwort
- Systemrücksetzung

Inhalt dieses Kapitels

Dieses Kapitel enthält die folgenden Themen:

Thema	Seite
Benutzerschnittstelle starten (NxS07100)	100
Arbeiten mit der Benutzerschnittstelle (NxS07100)	102
Starten der Benutzerschnittstelle (NxS17100)	107
Arbeiten mit der Benutzerschnittstelle (NxS17100)	109

Benutzerschnittstelle starten (NxS07100)

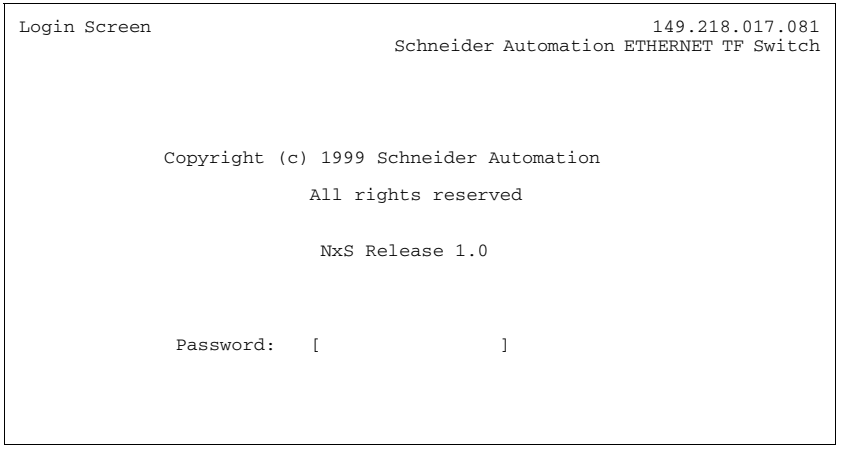
Übersicht

Führen Sie die folgenden Schritte aus, um die Benutzerschnittstelle zu starten und das Passwort einzugeben.

Schritt	Aktion	Kommentar
1	Drücken Sie nach dem Verbinden des Verwaltungsagenten mit einer VT100-Station über V.24 eine Taste.	Auf dem Bildschirm wird ein Fenster zum Eingeben des Passworts angezeigt. Nur ein einzelner Benutzer kann auf die Benutzerschnittstelle zugreifen.
2	Geben Sie das Passwort ein.	Die Standardvorgabe für das Passwort ist **private**. Sie können das Passwort später über die Benutzerschnittstelle oder die WWW-Schnittstelle ändern (siehe *Passwort, S. 106*). Bitte denken Sie daran, dass bei Passwörtern die Groß- und Kleinschreibung zu beachten ist.
3	Drücken Sie die **<EINGABETASTE>**.	Das Hauptmenüfenster wird angezeigt.

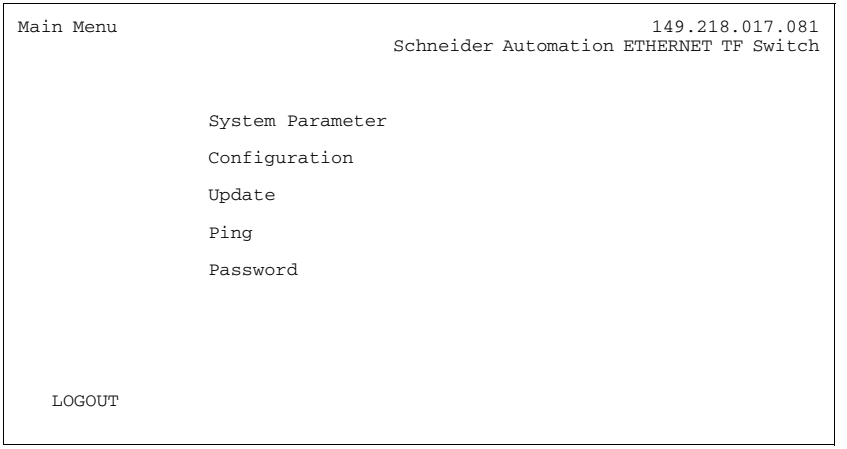
Anmelden an der Benutzer-schnittstelle

Die folgende Abbildung zeigt den Anmeldebildschirm der Benutzerschnittstelle.



Benutzer-schnittstellen-Hauptmenü

Die folgende Abbildung zeigt das Hauptmenü.



Arbeiten mit der Benutzerschnittstelle (NxS07100)

Grundlagen zum Arbeiten mit der Benutzerschnittstelle

- Verwenden Sie die Pfeiltasten oder die Tabulatortaste, um den Cursor zu bewegen.
- Um festgelegte Werte in einem Auswahlfeld zu ändern, drücken Sie die **Leertaste**.
- Die neuen Einstellung werden übernommen, wenn sich das Laufzeichen im Feld **APPLY** (ANWENDEN) befindet und die Eingabetaste gedrückt wird.
- Die unten stehende Zeile enthält einen Hilfetext für das gewählte Element.
- Um die Benutzerschnittstelle zu verlassen, wählen Sie im Hauptmenü die Option **LOGOUT** (ABMELDEN) und drücken die Eingabetaste.

Das Hauptmenü besteht aus fünf Untermenüs:

1. Systemparameter
2. Konfiguration
3. Aktualisierung
4. Ping
5. Passwort

Systemparameter

Dieses Menü dient zur Eingabe von

- IP-Adresse
- Subnet-Maske
- Gateway-IP-Adresse

um die MAC-Adresse des NxS anzuzeigen und das System neu zu starten.
In der folgenden Abbildung wird das Systemparameterfenster gezeigt.

```
System Parameter                                        149.218.017.081
                                        Schneider Automation ETHERNET TF Switch


                  IP Address       : [149.218.017.081]
                  Subnet Mask      : [255.255.240.0  ]
                  Default Gateway  : [0.0.0.0        ]

                  MAC Address      : 00:80:63:08:65:09









                  Reset            : < no reset >


MAIN MENU   APPLY
```

IP-Adresse

Geben Sie hier die IP-Adresse des Verwaltungsagenten ein. Die Standardeinstellung der Adresse ist 0.0.0.0.

Subnet-Maske

Wenn Sie mit einem großen Netzwerk arbeiten und Subnet-Masken verwenden, können Sie hier die Maske des Teilnetzes angeben, mit der Ihr Verwaltungsagent verbunden ist. Die Standardeinstellung der IP-Adresse ist 0.0.0.0.

Gateway-IP-Adresse

Geben Sie hier die IP-Adresse des Gateways ein, mit welcher der Verwaltungsagent andere Teilnetze adressieren soll. Wenn kein solches Gateway vorhanden ist, können Sie diese Eintrag auslassen. Die Standardeinstellung der IP-Adresse ist 0.0.0.0.

MAC-Adresse

In diesem Feld wird die MAC-Adresse des Geräts angezeigt.

Neustart

Um das System neu zu starten, wählen Sie die Rücksetzungszeile. Durch Drücken der **Leertaste** können Sie die Rücksetzungseinstellung von "keine Rücksetzung" auf "Rücksetzung" ändern. Nach dem Aktivieren der Option **APPLY** (ANWENDEN) führt der NxS einen Neustart aus.

Konfiguration

Der NxS hat zwei Konfigurationseinstellungen:

- Standardeinstellung
- Benutzerdefinierte Einstellung.

Mit Hilfe dieses Untermenüs kann eine benutzerdefinierte Konfiguration abgespeichert werden Diese Konfiguration kann beim Neustart automatisch geladen werden, oder nach dem Neustart und dem erneuten Laden der Standardeinstellungen.

Anhand einer Einstellung können Sie bestimmen, welche Konfigurationseinstellung nach einem Neustart aktiviert wird:

- Durch **Sperren** wird die Standardkonfiguration geladen.
- Durch **Freigeben** wird die benutzerdefinierte Konfiguration geladen.

Änderungen in diesem Fenster werden durch die Option **APPLY** (ANWENDEN) übernommen.

Die folgenden Abbildung zeigt den Konfigurationsbildschirm "Speichern/Laden".

```
Save/Load Configuration                                  149.218.017.081
                                      Schneider Automation ETHERNET TF switch




   Save/Load configuration:        <config-save>

   Load configuration after reset: <  Disable  >



   To save your current MIB-configuration apply with config-save.
   To load a saved MIB-configuration apply with config-load.
  Enabling the configuration loads a saved configuration after a systemstart.


MAIN MENU   APPLY
```

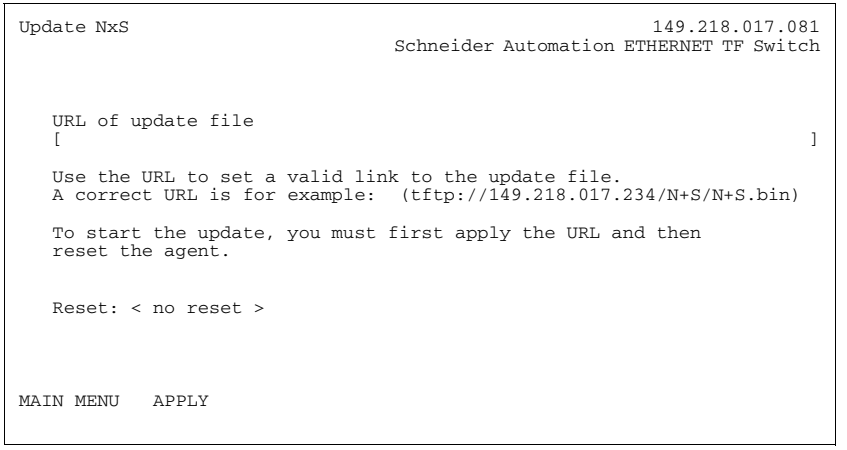
Aktualisierung

Bevor Sie die Software aktualisieren können, müssen Sie den genauen Standort (Pfadname) der Update-Datei kennen.

Schritt	Aktion
1	Geben Sie den korrekten Pfadnamen in das Feld **URL of update file** (URL der Aktualisierungsdatei) ein, und drücken Sie die **Eingabetaste**.
2	Legen Sie in der Zeile **Zurücksetzen** fest, ob der NxS unmittelbar nach dem Laden einer Aktualisierung oder zu einem späteren Zeitpunkt gestartet werden soll.
3	Wählen Sie die Option **Anwenden**, um die Aktualisierung zu laden. Sie wird nach einem Neustart aktiviert.

Aktualisieren des NxS

Die folgende Abbildung zeigt den Bildschirm "NxS aktualisieren".


Update NxS
149.218.017.081
Schneider Automation ETHERNET TF Switch
URL of update file
[ ]
Use the URL to set a valid link to the update file.
A correct URL is for example: (tftp://149.218.017.234/N+S/N+S.bin)
To start the update, you must first apply the URL and then reset the agent.
Reset: < no reset >
MAIN MENU APPLY

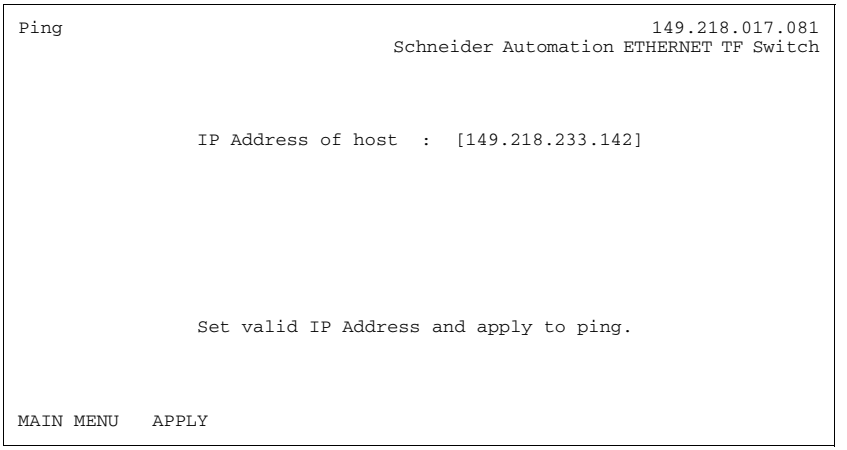
Ping

Im Menü Ping können Sie die Verfügbarkeit einer anderen Netzwerkstation prüfen.

Schritt	Aktion	Kommentar
1	Geben Sie im Feld **IP address of host** (IP-Adresse des Host) die IP-Adresse der gewünschten Station ein, und drücken Sie dann die **Eingabetaste**.	
2	Wählen Sie die Option **Anwenden**, um anhand von Ping festzustellen, ob die gewünschte Station verfügbar ist.	Je nach der Verfügbarkeit der Station erhalten Sie eine von zwei Antworten. • "Host aktiv" • "Host nicht aktiv"

Menü Ping

In der folgenden Abbildung wird das Menü Ping gezeigt.


Ping
149.218.017.081
Schneider Automation ETHERNET TF Switch
IP Address of host : [149.218.233.142]
Set valid IP Address and apply to ping.
MAIN MENU APPLY

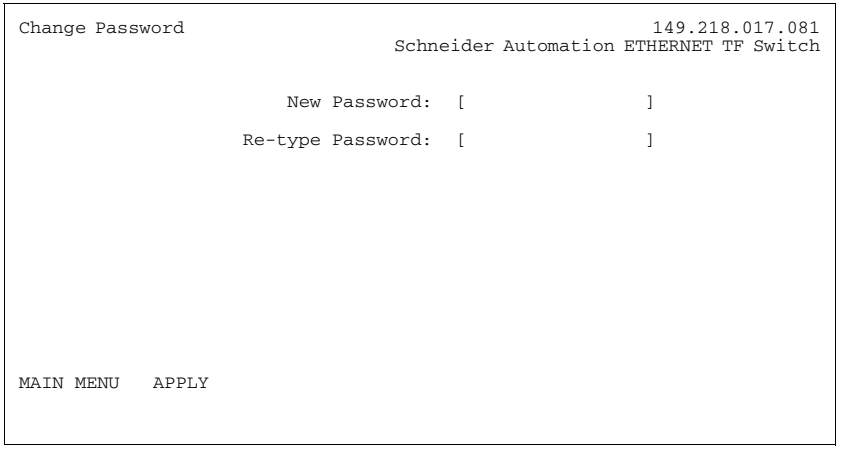
Passwort

Ändern Sie in diesem Untermenü das Passwort, um den NxS gegen unberechtigten Zugriff zu schützen.

Schritt	Aktion
1	Geben Sie das neue Passwort in das Feld **Neues Passwort** ein, und drücken Sie die **Eingabetaste**.
2	Wiederholen Sie den Eintrag des neuen Passworts im Feld **Retype password** (Passwort erneut eingeben), und drücken Sie die **Eingabetaste**.
3	Wählen Sie die Option **APPLY** (ANWENDEN), um das neue Passwort zu übernehmen, und drücken Sie die **Eingabetaste**.
4	Speichern Sie die Konfiguration, um sicherzustellen, dass das neue Passwort nach einem Neustart verfügbar ist (siehe *Konfiguration, S. 103*).

Menü "Passwort ändern"

In der folgenden Abbildung wird das Menü "Passwort ändern" gezeigt.



Starten der Benutzerschnittstelle (NxS17100)

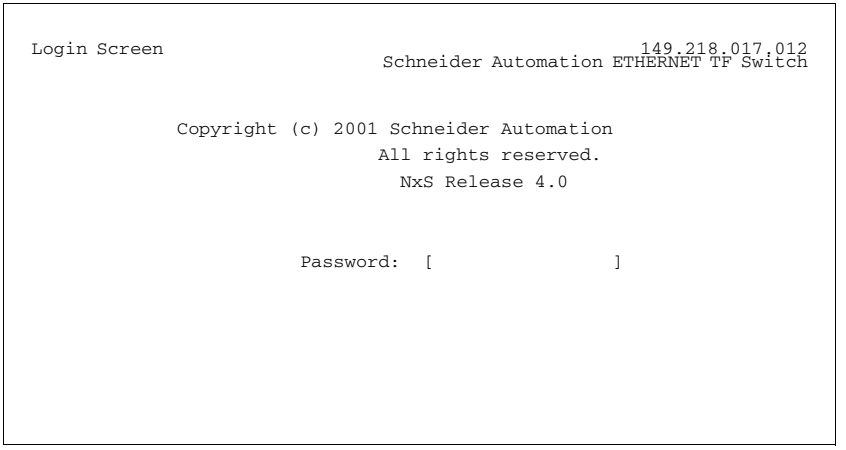
Übersicht

Führen Sie die folgenden Schritte aus, um die Benutzerschnittstelle zu öffnen und das Passwort einzugeben.

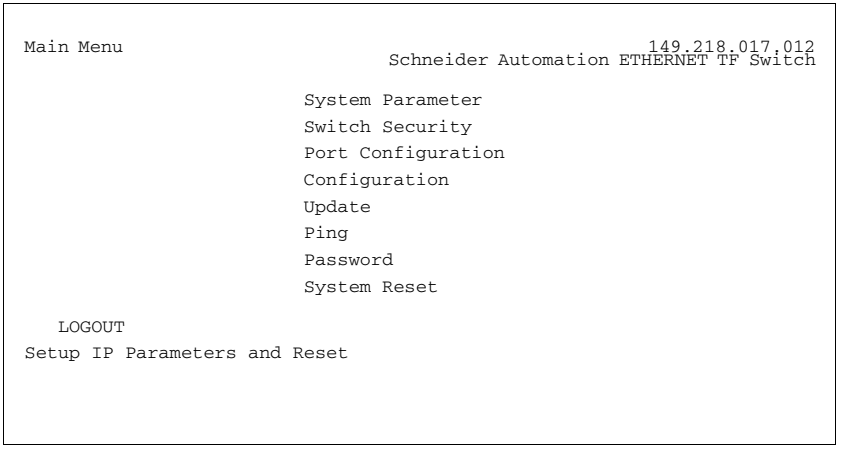
Schritt	Aktion	Kommentar
1	Drücken Sie nach dem Verbinden des Verwaltungsagenten mit einer VT100-Station über V.24 eine Taste.	Auf dem Bildschirm wird ein Fenster zum Eingeben des Passworts angezeigt. Nur ein einzelner Benutzer kann auf die Benutzerschnittstelle zugreifen.
2	Geben Sie das Passwort ein.	Die Standardvorgabe für das Passwort ist **private**. Sie können das Passwort später über die Benutzerschnittstelle oder die WWW-Schnittstelle ändern (siehe *Menü "Passwort ändern", S. 117*). Bitte denken Sie daran, dass bei Passwörtern die Groß- und Kleinschreibung zu beachten ist.
3	Drücken Sie die **<EINGABETASTE>**.	Das Hauptmenüfenster wird angezeigt.

Anmelden an der Benutzer-schnittstelle

In der folgenden Abbildung wird das Fenster zum Anmelden an der Benutzerschnittstelle gezeigt.



In der folgenden Abbildung wird das Hauptmenü gezeigt.



Arbeiten mit der Benutzerschnittstelle (NxS17100)

Grundlagen zum Arbeiten mit der Benutzer-schnittstelle

- Verwenden Sie die Pfeiltasten oder die Tabulatortaste, um den Cursor zu bewegen.
- Um festgelegte Werte in einem Auswahlfeld zu ändern, drücken Sie die **Leertaste**.
- Die neuen Einstellung werden übernommen, wenn sich das Laufzeichen im Feld **APPLY** (ANWENDEN) befindet und die Eingabetaste gedrückt wird.
- Die unten stehende Zeile enthält einen Hilfetext für das gewählte Element.
- Um die Benutzerschnittstelle zu verlassen, wählen Sie im Hauptmenü die Option **LOGOUT** (ABMELDEN) und drücken die Eingabetaste.

Das Hauptmenü besteht aus sieben Untermenüs:

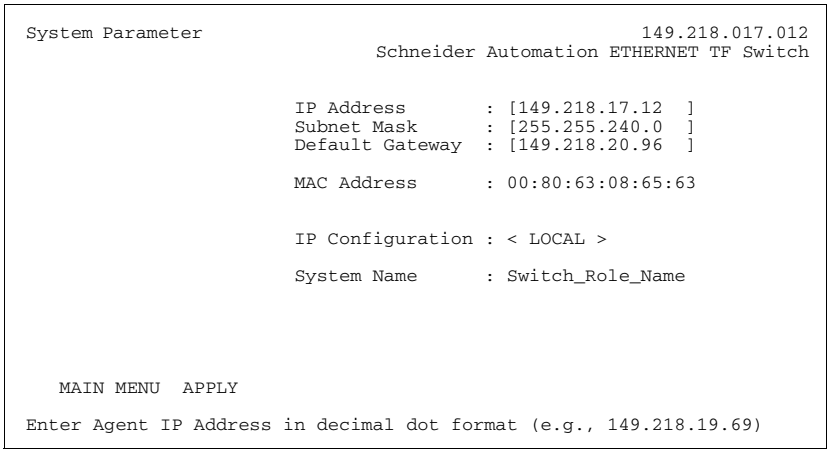
1. Systemparameter
2. Switchsicherheit
3. Portkonfiguration
4. Konfiguration
5. Aktualisierung
6. Ping
7. Passwort

System-parameter

Über dieses Menü kann die

- IP-Adresse
- Subnet-Maske
- Gateway-IP-Adresse

eingegeben werden, um die MAC-Adresse des NxS anzuzeigen und BOOTP/DHCP zu aktivieren/deaktivieren.
In der folgenden Abbildung wird das Systemparameterfenster gezeigt.


System Parameter
149.218.017.012
Schneider Automation ETHERNET TF Switch
IP Address : [149.218.17.12]
Subnet Mask : [255.255.240.0]
Default Gateway : [149.218.20.96]
MAC Address : 00:80:63:08:65:63
IP Configuration : < LOCAL >
System Name : Switch_Role_Name
MAIN MENU APPLY
Enter Agent IP Address in decimal dot format (e.g., 149.218.19.69)

IP-Adresse Geben Sie hier die IP-Adresse des Verwaltungsagenten ein. Die Standardeinstellung der Adresse ist 0.0.0.0.

Subnet-Maske Wenn Sie mit einem großen Netzwerk arbeiten und Subnet-Masken verwenden, können Sie hier die Maske des Teilnetzes angeben, mit dem Ihr Verwaltungsagent verbunden ist. Die Standardeinstellung der IP-Maske ist 0.0.0.0.

Gateway-IP-Adresse Geben Sie hier die IP-Adresse des Gateways ein. Wenn kein solches Gateway vorhanden ist, können Sie diese Eintrag auslassen. Die Standardeinstellung der IP-Adresse ist 0.0.0.0.

MAC-Adresse In diesem Feld wird die MAC-Adresse des Geräts angezeigt.

Neustart Um das System neu zu starten, wählen Sie die Rücksetzungszeile. Durch Drücken der **Leertaste** können Sie die Rücksetzungseinstellung von "keine Rücksetzung" auf "Rücksetzung" ändern. Nach dem Aktivieren der Option **APPLY** (ANWENDEN) führt der NxS einen Neustart aus.

IP-Konfiguration Führen Sie die folgenden Schritte aus, um eine IP-Konfiguration auszuführen.

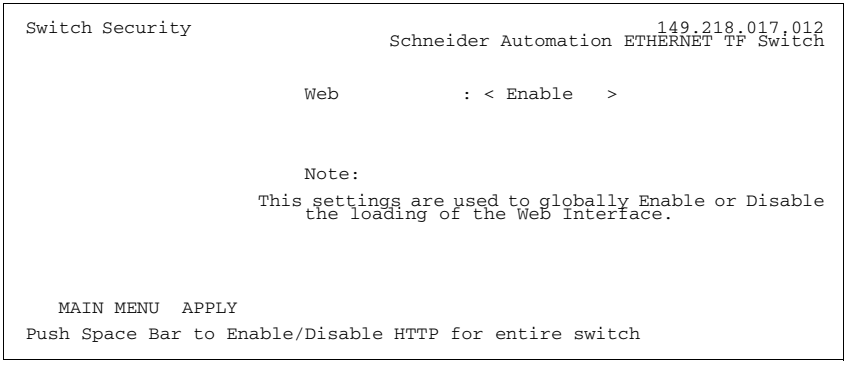
Schritt	Aktion	Kommentar
1	Wählen Sie den gewünschten IP-Konfigurationsmodus.	Durch Drücken der **Leertaste** werden die folgenden Optionen bereitgestellt: • Lokal • BOOTP- • DHCP-Protokoll
2	Wählen Sie **APPLY** (ANWENDEN).	Der Modus ist aktiviert. (Siehe *Grundeinstellungen, S. 28*.)
3	Weisen Sie dem NxS den von Ihnen gewählten Systemnamen zu.	(Siehe *DHCP-Protokoll, S. 29*.)

Switchsicherheit

In diesem Menü wird der Zugriff auf die webbasierte Verwaltung konfiguriert.

- Durch **Sperren** wird der Zugriff über die webbasierte Verwaltung nicht gestattet.
- Durch **Freigeben** wird der Zugriff über die webbasierte Verwaltung ermöglicht.

In der folgenden Abbildung wird das Menü Switchsicherheit gezeigt.


Switch Security
149.218.017.012
Schneider Automation ETHERNET TF Switch
Web : < Enable >
Note:
This settings are used to globally Enable or Disable the loading of the Web Interface.
MAIN MENU APPLY
Push Space Bar to Enable/Disable HTTP for entire switch

Port-konfiguration

Anhand der folgenden Schritte wird die Portkonfiguration ausgeführt.

Schritt	Aktion	Kommentar
1	Geben Sie die Portnummer ein, und drücken Sie die **Eingabetaste**.	
2	Wählen Sie den Status.	Statusoptionen: • Durch **Sperren** wird der Port gesperrt. • Durch **Freigeben** wird der Port freigegeben.
3	Wählen Sie die Übertragungsgeschwindigkeit.	Optionen der Übertragungsgeschwindigkeit: • Durch **automatische Einstellung** wird der Port für die automatische Einstellung freigegeben. • **10MHDX** - 10 Mbit/s, Halbduplex. • **10MFDX** - 10 Mbit/s, Duplex. • **100MHDX** - 100 Mbit/s, Halbduplex. • **100MFDX** - 100 Mbit/s, Duplex.
4		

Menü Port-konfiguration

In der folgenden Abbildung wird das Menü Portkonfiguration gezeigt.

```
Port Configuration                                    149.218.017.012
                                  Schneider Automation ETHERNET TF Switch

  Port: 1
  State: <Enable   >  Set Speed:    <autonegotiate >
  Link:  Down         Actual Speed: 10MHDX


  Note:
  Apply changes the settings.
  Refresh updates the screen.


   MAIN MENU   APPLY   REFRESH
Type in port number and press enter
```

Konfiguration

Der NxS hat zwei Konfigurationseinstellungen:

- Standardeinstellung
- Benutzerdefinierte Einstellung.

Dieses Untermenü bietet die Option zum Speichern einer benutzerdefinierten Konfiguration. Diese Konfiguration kann beim Neustart automatisch geladen werden, oder nach dem Neustart und dem erneuten Laden der Standardeinstellungen.

Mit **Load after reset** (Laden nach Rücksetzung) können Sie bestimmen, welche Konfigurationseinstellung nach einem Neustart aktiviert wird.

- Durch **Standard** wird die Standardkonfiguration geladen.
- Durch **lokal** wird die benutzerdefinierte Konfiguration geladen.
- Durch **remote** (dezentral) wird die benutzerdefinierte Konfiguration aus der Konfigurationsdatei auf dem TFTP-Server geladen.

Durch **Laden** wird bestimmt, welche Konfiguration geladen werden soll.

- Durch **lokal** wird die benutzerdefinierte Konfiguration aus dem Flash-Speicher geladen.
- Durch **remote** (dezentral) wird die benutzerdefinierte Konfiguration aus der Konfigurationsdatei auf dem TFTP-Server geladen.

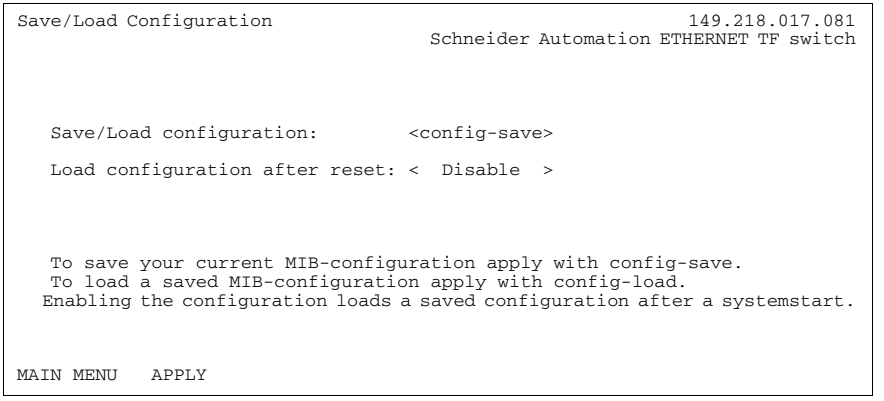
Durch **Speichern** wird bestimmt, wo die Konfigurationseinstellung gespeichert wird.

- Durch **lokal** wird die benutzerdefinierte Konfiguration im Flash-Speicher gespeichert.
- Durch **remote** (dezentral) wird die benutzerdefinierte Konfiguration als Konfigurationsdatei auf dem TFTP-Server gespeichert.

Änderungen in diesem Fenster werden durch die Option **APPLY** (ANWENDEN) übernommen.

Der Pfad zum Speichern der Konfigurationsdaten wird in der Zeile "URL" angezeigt. Da TFTP nicht fähig ist, eine neue Datei zu erstellen, erstellen Sie eine leere Datei auf dem TFTP-Server, bevor Sie die Option "Save to URL" (In URL speichern) ausführen.

In der folgenden Abbildung wird das Speichern/Laden-Konfigurationsfenster gezeigt.


Save/Load Configuration
149.218.017.081
Schneider Automation ETHERNET TF switch
Save/Load configuration: <config-save>
Load configuration after reset: < Disable >
To save your current MIB-configuration apply with config-save.
To load a saved MIB-configuration apply with config-load.
Enabling the configuration loads a saved configuration after a systemstart.
MAIN MENU APPLY

Auf einem TFTP-Server speichern

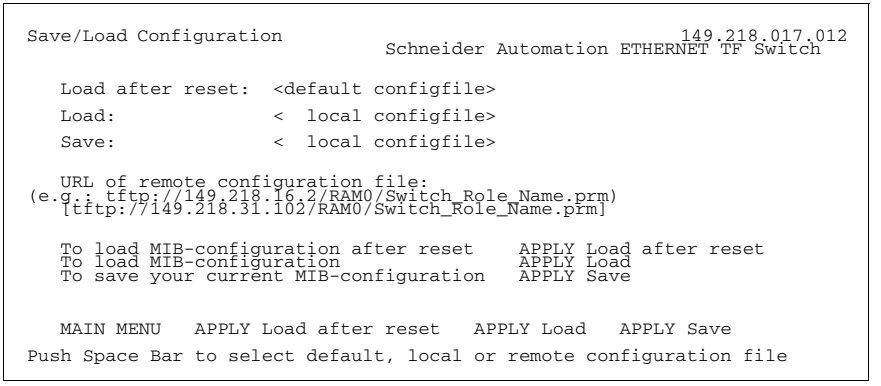
Gehen Sie beim Speichern auf einem TFTP-Server wie beschrieben vor.

Schritt	Aktion
1	Öffnen Sie mit einem Editor eine neue Datei.
2	Speichern Sie die leere Datei unter dem jeweiligen Pfad des TFTP-Servers einschließlich Dateiname, z.B. **RAM0/Switch_Role_Name.prm**
3	Geben Sie auf der Zeile "URL" den Pfad des TFTP-Servers ein, z.B. **tftp://149.218.076.214/RAM0/Switch_Role_Name.prm**.

Menü "Konfiguration speichern/laden"

Hinweis: Die Konfigurationsdatei enthält alle Konfigurationsdaten einschließlich Passwort. Legen Sie darum die Zugriffsberechtigungen für den TFTP-Server entsprechend fest.

In der folgenden Abbildung wird das Menü "Konfiguration speichern/laden" gezeigt.



Aktualisierung

Ehe Sie die Software aktualisieren können, müssen Sie den genauen Speicherort bzw. den Pfad der Aktualisierungsdatei kennen.

Schritt	Aktion
1	Geben Sie den korrekten Pfadnamen in das Feld **URL of update file** (URL der Aktualisierungsdatei) ein, und drücken Sie die **Eingabetaste**.
2	Legen Sie in der Zeile **Zurücksetzen** fest, ob der NxS unmittelbar nach dem Laden einer Aktualisierung oder zu einem späteren Zeitpunkt gestartet werden soll.
3	Wählen Sie die Option **Anwenden**, um die Aktualisierung zu laden. Sie wird nach einem Neustart aktiviert.

Menü "Software aktualisieren"

In der folgenden Abbildung wird das Menü "Software aktualisieren" gezeigt.

```
Update software                                          149.218.017.012
                                  Schneider Automation ETHERNET TF Switch


   URL of update file:
   [tftp://149.218.16.5/nxs/k3_30_01.bin                                ]

   Use the URL to set a valid link to the update file.
   A correct URL is for example:  (tftp://149.218.16.2/nxs/nxs.bin)

   To start the update, you must first apply the URL and then
   reset the agent.


   Reset :  < no reset >




   MAIN MENU   APPLY
Enter URL of remote update file
```

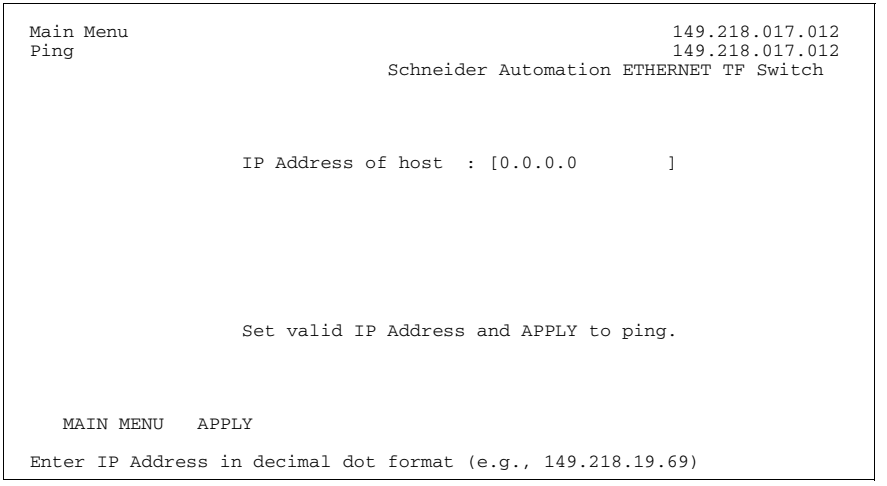
Ping

Im Menü Ping können Sie die Verfügbarkeit einer anderen Netzwerkstation prüfen.

Schritt	Aktion	Kommentar
1	Geben Sie im Feld **IP address of the host** (IP-Adresse des Host) die IP-Adresse der gewünschten Station ein, und drücken Sie dann die **Eingabetaste**.	
2	Wählen Sie die Option **Anwenden**, um anhand von Ping festzustellen, ob die gewünschte Station verfügbar ist.	Je nach der Verfügbarkeit der Station erhalten Sie eine von zwei Antworten. • "Host aktiv" • "Host nicht aktiv"

Menü Ping

In der folgenden Abbildung wird das Menü Ping gezeigt.


Main Menu 149.218.017.012
Ping 149.218.017.012
Schneider Automation ETHERNET TF Switch
IP Address of host : [0.0.0.0]
Set valid IP Address and APPLY to ping.
MAIN MENU APPLY
Enter IP Address in decimal dot format (e.g., 149.218.19.69)

Passwort

Ändern Sie in diesem Untermenü das Passwort, um den NxS gegen unberechtigten Zugriff zu schützen.

Schritt	Aktion
1	Geben Sie das alte Passwort in das Feld **Altes Passwort** ein, und drücken Sie die **Eingabetaste**.
2	Geben Sie das neue Passwort in das Feld **Neues Passwort** ein, und drücken Sie die **Eingabetaste**.
3	Wiederholen Sie den Eintrag des neuen Passworts im Feld **Retype password** (Passwort erneut eingeben), und drücken Sie die **Eingabetaste**.
4	Wählen Sie die Option **APPLY** (ANWENDEN), um das neue Passwort zu übernehmen, und drücken Sie die **Eingabetaste**.
5	Speichern Sie die Konfiguration, um sicherzustellen, dass das neue Passwort nach einem Neustart verfügbar ist (siehe *Konfiguration, S. 113*).

Menü "Passwort ändern"

In der folgenden Abbildung wird das Menü "Passwort ändern" gezeigt.

```
Change Password                                          149.218.017.012
                                  Schneider Automation ETHERNET TF Switch

                          Old Password: [                ]
                          New Password: [                ]
                       Re-type Password: [                ]









   MAIN MENU  APPLY
Type in old case sensitive password (up to 16 characters)
```

System-rücksetzung

Führen Sie die folgenden Schritte aus, um den NxS zurückzusetzen.

Schritt	Aktion
1	Wählen Sie die Zeile **Confirm Reset** (Rücksetzung bestätigen).
2	Drücken Sie die **Leertaste**, um die Einstellung von **Nein** auf **Ja** zu ändern.
3	Wählen Sie **APPLY** (ANWENDEN), um den NxS zurückzusetzen.

Menü System-rücksetzung

In der folgenden Abbildung wird das Menü Systemrücksetzung gezeigt.

```
System Reset                                             149.218.017.012
                                  Schneider Automation ETHERNET TF Switch

            WARNING:
                     This will cause all connectivity to
                     the switch to be lost until the switch
                     has rebooted.

            Confirm Reset:  < No  >









   PREV MENU  APPLY
Push Space Bar to select 'yes' and reset the switch
```

Index

Nummern

100-Mbit/s-Verbindung
einrichten der Hauptleitung, 23
2-poliger DIP-Schalter
Abbildung, 20
499NES07100
Abbildung, 71
499NES17100
Abbildung, 14
499NESx7100
Funktionen, 14
499NOS17100
Abbildung, 15
499NOSx7100
Beschreibung, 15
Funktionen, 16
5-polige Anschlussklemmleiste
Abbildung, 21

A

Adressumsetzungsgruppe, 85
Aktualisierungen, 114
Alarmanzeige
Abbildung, 69
Automationstechnologie
Ethernet-Standard, 10
Trends, 10
Automatische Einstellung
Lieferzustand, 23
automatische Einstellung
Beschreibung, 52
Automatische Polarität, 23

B

Benutzergruppen-Gruppe, 98
Benutzerschnittstelle
Anmeldebildschirm, 100
Hauptmenü, 101
starten, 100
Benutzerschnittstelle (4.0), 107
Benutzerschnittstelle (NxS07100)
arbeiten mit, 102
Benutzerschnittstelle (NxS17100), 109
Bit-Notierung
Abbildung, 35
BOOTP-Prozess, 28
Abbildung, 30

C

ConneXium Fast Ethernet-Switch
Verwendung in industrieller Automation, 10
ConneXium Fast-Ethernet-Switch
Beschreibung, 11
Funktionen, 11
mit SNMP Verwaltungsagent, 11

D

Dateikartensystem
Funktionen, 73

Datenblockvermittlung
Kennzeichnung, 54
lernen von Adressen, 54
Mehrfachadressen-Fähigkeit, 54
Prioritätensetzung, 54
Speichern und Weiterleiten, 54
Dezentrale Steuersysteme
Verwendung in Industrieautomation, 10
dot1dBridge, 92
Dynamic Host Configuration Protocol (DHCP), 29

E

Ethernet Ring
Verwendung in industrieller Automation, 10

F

Fehlerkontakt
Überwachungsfunktion, 21

G

Gateway-IP-Adresse
eingeben, 34
Gateways, 109
Gehäuse
öffnen, 18
generische Objektklasse, 80
Gerätegruppe, 95
Gerätestatus
LED-Anzeigen, 53
Geschirmte und foliengeschirmte Twisted-Pair-Segmente
verbinden mit 4999NESx7100, 14
Geschirmter Erdleiter
anschließen, 18
GMRP, 59
Abbildung, 59
aktivieren über SNMP, 60

H

Herkunftsadresse, 37

I

ICMP-Gruppe, 87
INET-Hintergrundroutine
neuinitialisieren unter HP, 41
neuinitialisieren unter SunOS, 41
IP-Adresse, 109
Beschreibung, 35
Eingabe über Station, 34
Eingabefolge, 33
eingeben, 28
Klassifizierung, 35
Standardwert, 34
IP-Adresse mit Teilnetz-Zuweisung
Abbildung, 36
IP-Gruppe, 86
ISO/OSI, 38

K

Kommunikation mit Netzverwaltungsstation, 61
Konfiguration
Einstellungen, 103
nach Neustart, 103
Konfigurationen, 34, 113
Konfigurationsbildschirm "Speichern/Laden", 103
Kontaktunterbrechungen
Ursachen, 21

L

Leitungsinstallation, 26
Leitungsüberwachung
mit Lichtwellenleitern, 52
mit Twisted-Pair, 52

M

MAC-Adresse, 38, 109
MAU-Verwaltungsgruppe, 94

MDI-X
Äquivalente der Stiftbelegung, 23
MIB
Abkürzungen, 81
Baumstruktur, 82
Beschreibung, 80
Syntax, 81
mittlere bis große Netzwerke
konfigurieren mit ConneXium-Switches, 11
Montage
Vorgehensweise, 22
Multicasting, 59

N

Nebenbezeichner, 80
Netzwerkadresse, 35
Netzwerkkonfiguration
Abbildung, 74
benutzerdefinierte Konfigurationen speichern, 74
Parameter zuweisen, 74
Passwort ändern, 77
Software aktualisieren, 76
speichern auf einem TFTP-Server, 75
Netzwerkmaske, 35, 109
Abbildung, 36
Geräte Teilnetzen zuweisen, 36
Netzwerkverwaltung
aktivieren, 28
Neustart, 113
Normalmodus
Zustände, 21
NsX-Startseite
Einzelanschlusskonfigurationi, 73
NsX-Startseiten
Anschlussregistersymbole, 72
NxS
anmelden, 67
bedienen über das Web, 69
Buskonfiguration, 55
Demontage, 26
grafische Konfiguration, 65
IP-Adressen konfigurieren, 28
redundante Kopplung von Netzwerksegmenten, 57
Redundanz-Manager-Funktion, 56
starten, 27
Startseite, 68, 69
verhindern unberechtigter Zugriffe, 62
verwalten über das Web, 65
NxS-Bildschirm aktualisieren, 104
NxS-Startseite
aktualisieren, 71
Alarmzustand, 69
Aufzeichnung, 70
Ereignisspeicher-Anzeige, 70
Konfiguration, 71
Registerkarte Anschluss, 71
System-Ereignisspeicher, 70
Systemparameter-Anzeige, 70

O

Objektbeschreibung, 80
Objekt-ID, 80
Objektklasse, 80

P

Passwörter, 34, 106, 107, 116
Port-Sicherheit
Einstellungen, 61
Überwachung, 61
Port-Status
LED-Anzeigen, 53
private MIB, Definition, 95

Q

Qualifiziertes Personal
Anforderungen für, 19

R

Redundanz
Buskonfiguration, 55
koppeln von Netzwerksegmenten, 57
redundante Ringkonfiguration, 56

Redundanz-Manager, 20
RMON-Gruppe, 90

S

Schnittstellengruppe, 85
Sicherheits-Kleinstspannung
  Auswirkung auf Verbindungsaufbau, 18
SNMP, 61
SNMP-Gruppe, 89
SNMP-Traps
  Definition, 62
  Typen, 63
Software-Aktualisierungen
  Anforderungen, 39
Standby-Modus
  Zustände, 21
Standby-Port, 23
Standby-Schnittstelle
  Abbildung der Stiftbelegung, 24
Steuerungskabel
  Abbildung, 24
  maximale Länge bestimmen, 24
Switch-Software
  im Flash-Speicher, 39
System Monitor 1
  ändern der Baudrate, 47
  beenden, 47
System neu starten, 103, 110
Systemgruppe, 83
Systemgruppenobjekte, 84
Systemmonitor 1
  Abbildung des Hauptmenüs, 45
  aktualisieren des Betriebssystems, 44, 45
  starten des Betriebssystems, 46
  Startphase, 44
Systemmonitor 2
  Betriebssystemaktualisierung, 50
  Hauptmenü, 49
  Softwareaktualisierung, 49
  Startphase, 48
Systemparameter, Bildschirm, 102

T

TCP, 88
TCP-Gruppe, 88
TFTP-Prozess
  einrichten, 39
  installieren auf HP-Workstations, 40
  prüfen, 40
  Status-Bestimmung unter HP, 41
  Status-Bestimmung unter SunOS, 41
TFTP-Server
  Ablaufplan zur Einrichtung, 42
  Verzeichnisstruktur, 43
TFTP-Sicherheit, 75
TP/TX-Schnittstelle
  Abbildung, 23
Trap-Nachricht
  Definition, 62
Trap-Zieltabelle
  konfigurieren, 62

U

Übertragungsparameter, 34
UDP-Gruppe, 88
Umgebungsbedingungen
  Betrieb des Geräts, 19

V

V.24, 107
V.24-Schnittstelle
  Abbildung, 25
  anschließen, 25
Versorgungsspannung
  anschließen, 21
Verwaltungsagent, 99
Verwaltungsgruppe, 97
VLAN-Tag
  Beschreibung, 54
VT100, 107
VT100-Terminal
  Einstellungen, 25

W

Webbasierte Schnittstelle
aktivieren, 66

Z

Zieladresse, 37, 105, 115
Zieltabelle
konfigurieren, 62